

The ServiceNow logo is displayed in white lowercase letters on a dark blue background. The background of the entire top half of the page features a dynamic, abstract pattern of glowing blue and cyan light streaks that radiate from a bright point on the right side, creating a sense of motion and energy.

servicenow®

10/16/2018

10/16/2018

## **Istanbul Governance, risk, and compliance (GRC)**

Some examples and graphics depicted herein are provided for illustration only. No real association or connection to ServiceNow products is intended or should be inferred.

---

If you have comments about this documentation, submit your feedback to:  
[docfeedback@servicenow.com](mailto:docfeedback@servicenow.com)

Please read the ServiceNow Terms of Use Privacy Statement at  
[www.servicenow.com/privacy-statement.html](http://www.servicenow.com/privacy-statement.html)

Company Headquarters  
2225 Lawson Lane  
Santa Clara, CA 95054  
United States  
(408)501-8550

# Contents

<b>Governance, Risk, and Compliance (GRC)</b> .....	<b>4</b>
Policy and Compliance Management.....	5
Activate Policy and Compliance Management.....	6
Dependency modeling and mapping.....	13
Compliance.....	13
Policies and procedures.....	20
GRC profile scoping.....	31
Use UCF Common Controls Hub to manage compliance frameworks.....	36
Controls.....	49
GRC issues management.....	58
GRC continuous monitoring.....	60
GRC PA Indicators.....	63
Policy and Compliance Administration.....	66
Risk Management.....	67
Activate Risk Management.....	68
Risk Management process.....	78
Risk Overview.....	78
GRC Workbench.....	79
Risk Library.....	88
GRC profile scoping.....	91
Risk Register.....	95
GRC issues management.....	105
GRC continuous monitoring.....	107
GRC PA Indicators.....	111
Risk Management Administration.....	114
Audit Management.....	115
Activate Audit Management.....	115
Engagement Overview.....	123
Engagement Workbench.....	125
Engagements.....	126
GRC profile scoping.....	131
Audit tasks.....	136
Audit testing.....	143
GRC continuous monitoring.....	145
GRC issues management.....	148
Audit Management Administration.....	150
Governance, Risk, and Compliance (GRC) - Legacy.....	151
Legacy migration.....	152
Activate GRC Risk - Legacy.....	165
What is GRC? - Legacy.....	170
Risk Management overview - Legacy.....	274
Activate Governance, Risk, and Compliance (GRC) - Legacy.....	286
<b>Index</b> .....	<b>287</b>

# Governance, Risk, and Compliance (GRC)

The ServiceNow® GRC application contains three main products: Policy and Compliance Management, Risk Management, and Audit Management. The legacy GRC (com.snc.governance) plugin has been deprecated. Instances upgraded from a previous release can continue using legacy GRC, but the plugin is not available for activation. The GRC: Performance Analytics Premium Integration plugin provides an integration between Performance Analytics and the Risk Management and Policy and Compliance Management applications, providing more insight into organizational risk and compliance performance. The GRC Workbench plugin gives GRC administrators a graphical interface to create profile and risk dependencies enabling consistent risk mapping and modeling across the enterprise.



**Figure 1: GRC products**

The GRC-related applications allow your organization to:

- Manage issues to track remediation or issue exception
- Document and publish policies
- Download and import UCF content
- Utilize controls and mitigate risk
- Assess risk exposure
- Continuously monitor risks and controls
- Plan and conduct internal audits

## Notes about GRC plugins

- Whenever any of the GRC plugins are activated, both the GRC: Profiles [com.sn\_grc] plugin and the GRC: Common [com.sn.grc.common] plugins are automatically activated, providing core components and a common architecture for all GRC applications.

- All three GRC applications can be configured for mobile applications using the basic ServiceNow platform capabilities.
- Although Audit Management does not require the activation of the Policy and Compliance Management or Risk Management plugins, the functionality and features in the audit application are more robust if all three GRC plugins are activated.

## GRC roles

The GRC applications provide a set of ServiceNow roles that are personas for GRC professionals. These roles provide permissions to perform work and may contain other roles.

**Table 1: GRC roles**

Group	Description	Examples
Governance	Approves GRC documents	Board of Directors, Executive Staff
Specialized administrators	Sets criteria for using GRC	sn_compliance.admin, sn_risk.admin, sn_audit.admin
Managers	Perform all actions except those reserved for admins	sn_compliance.manager, sn_risk.manager, sn_audit.manager
Users	Own specific items, submit requests, and manage their own tasks, access public pages, take surveys, and use Live Feed and Chat.	sn_compliance.user, sn_risk.user, sn_audit.user

## Notes about integrations with UCF

- Users must have a UCF Common Controls Hub account to create shared lists and import them into ServiceNow®
- The UCF common controls functionality is not automatically turned on by activating Policy and Compliance Management. The GRC: Compliance UCF plugin must be activated and users must have a UCF Common Controls Hub account to create shared lists and import them into ServiceNow®

## Policy and Compliance Management

The ServiceNow® Policy and Compliance Management product provides a centralized process for creating and managing policies, standards, and internal control procedures that are cross-mapped to external regulations and best practices. Additionally, the application provides structured workflows for the identification, assessment, and continuous monitoring of control activities.

The GRC: Policy and Compliance Management (com.sn\_compliance) plugin is available as a separate subscription and requires activation.

Explore

Set up

Administer

- [GRC Common Release notes](#)

- [Policy and Compliance Release Notes](#)
- [Upgrade to Istanbul](#)
- [Activate Policy and Compliance Management](#) on page 6
- [Configure Policy and Compliance Management](#) on page 7
- [Policy and Compliance Administration](#) on page 66
- [GRC continuous monitoring](#) on page 60

## Use

- [Dependency modeling and mapping](#) on page 13
- [Attestation designer](#) on page 55

## Develop

- [Developer training](#)
- [Developer documentation](#)
- [Components installed with Policy and Compliance Management](#) on page 7

## Integrate

- [Use UCF Common Controls Hub to manage compliance frameworks](#) on page 36
- [GRC PA Indicators](#) on page 63

## Troubleshoot and get help

- [Ask or answer questions in the GRC community](#)
- [Search the HI Knowledge Base for known error articles](#)
- [Contact ServiceNow Support](#)

## Activate Policy and Compliance Management

The GRC: Policy and Compliance Management (com.sn\_compliance) plugin is available as a separate subscription.

Role required: admin

This plugin includes demo data and activates related plugins if they are not already active.

1. Navigate to [System Definition Plugins](#) .
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

If the plugin has optional features that are not functional because other plugins are inactive, those plugins are listed. A warning states that some files are not installed. If you want the optional features to be installed, cancel this activation, activate the necessary plugins, and then return to activating the plugin.

4. If available, select the Load demo data check box.

Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.

5. Click Activate.

To use the UCF import application, activate the UCF Import (com.sn\_comp\_ucf ) plugin.

## Configure Policy and Compliance Management

System and compliance administrators in the global domain can set properties to determine how the system defines the Policy and Compliance Management application.

Role required: admin, sn\_compliance.admin, sn\_compliance.developer

Compliance Administrators can set all the same properties except the Name of the assessment metric type that is used for attestations.

Administrators in domains lower than the global domain can view the Properties screen, but cannot modify the settings.

---

**Note:** A message appears at the top of the form This record is in the Policy and Compliance application, but <scope> is the current application to ensure that you are in the correct application scope.

---

1. Navigate to Policy and Compliance Administration Properties .
2. Fill in the fields on the form, as appropriate. See [Properties installed with Policy and Compliance Management](#) on page 8 for property descriptions.
3. Click Save.

## Components installed with Policy and Compliance Management

Activating the Policy and Compliance Management (com.sn\_compliance) plugin adds or modifies several tables, user roles, and other components.

### Tables installed with Policy and Compliance Management

Policy and Compliance Management adds the following tables.

Table	Description
Authority Document [sn_compliance_authority_document]	Extends the Document [sn_grc_document] table and stores all Authority Documents.
Control [sn_compliance_control]	Extends the Item [sn_grc_item] table and stores all controls.
Policy [sn_compliance_policy]	Extends the Document [sn_grc_document] table and stores all policies.
Article Template [sn_compliance_article_template]	Used to format the policy text contained in a policy record when publishing the policy to the Knowledge Base (KB).
Citation [sn_compliance_citation]	Extends the Content [sn_grc_content] table and stores all citations.
Policy to Profile Type [sn_compliance_m2m_policy_profile_type]	Extends Document to Profile Type [sn_grc_m2m_document_profile_type] and is a many-to-many relationship table that is used to manage the relationships between policies and profile types.

Table	Description
Policy Statement to Citation [sn_compliance_m2m_statement_citation]	Is a many-to-many relationship table that is used to manage relationships between policy statements and their related citations.
Policy Statement to Profile Type [sn_compliance_m2m_statement_profile_type]	Extends Content to Profile Type [sn_grc_m2m_content_profile_type] and is a many-to-many relationship table that is used to manage the relationships between policy statements and profile types.
Policy Statement [sn_compliance_policy_statement]	Extends the Content [sn_grc_content] table and stores all policy statements.

**Note:** All additional tables installed by the dependent plugins are also needed for Risk Management.

## Properties installed with Policy and Compliance Management

Policy and Compliance Management adds the following properties.

Name	Description
States for which the control is active (the first state is the default active state) sn_compliance.active_states	Compliance administrators can change this setting. <ul style="list-style-type: none"> <li>Type: string</li> <li>Default value: draft, assess, review, monitor</li> <li>Location: Policy and Compliance Administration Properties</li> </ul>
States for which control is inactive (the first state is the default inactive) sn_compliance.closed_states	Compliance administrators can change this setting. <ul style="list-style-type: none"> <li>Type: string</li> <li>Default value: retired</li> <li>Location: Policy and Compliance Administration Properties</li> </ul>
Name of the assessment metric type that is used for attestations sn_compliance.default_attestation	System administrators can change this setting. <ul style="list-style-type: none"> <li>Type: string</li> <li>Default value: GRC Attestation</li> <li>Location: Policy and Compliance Administration Properties</li> </ul>
sn_compliance.glide.script.block.client.globals	<ul style="list-style-type: none"> <li>Type: true or false</li> <li>Default value: false</li> <li>Location: Policy and Compliance Administration Properties</li> </ul>



Name	Description
Name of the knowledge base used to publish Policy articles sn_compliance.knowledge_base	Compliance administrators can change this setting. <ul style="list-style-type: none"> <li>Type: string</li> <li>Default value: Governance, Risk, and Compliance</li> <li>Location: Policy and Compliance Administration Properties</li> </ul>

## Roles installed with Policy and Compliance Management

GRC: Policy and Compliance Management adds the following roles.

Role title [name]	Description	Contains roles
Compliance Reader [sn_compliance.reader]	Contains the reader role in sn_grc scopes. In addition to the inherited permissions, the compliance reader can be assigned profile types, profiles, indicators templates, indicators and issues.	<ul style="list-style-type: none"> <li>sn_grc.reader</li> </ul>
Compliance User [sn_compliance.user]	Contains the reader and user roles in sn_grc scopes, and the reader role in the Policy and Compliance Management application. In addition to the inherited permissions, the compliance user can be assigned controls, and has read-only access to the Risk Management application and modules.	<ul style="list-style-type: none"> <li>sn_grc.reader</li> <li>sn_grc.user</li> <li>sn_compliance.reader</li> </ul>
Compliance Manager [sn_compliance.manager]	Contains the reader, user, and manager roles in sn_grc scopes, and the reader and user roles in the Policy and Compliance Management application. In addition to the inherited permissions, the compliance manager can create authority documents, citations, policies, policy statements, and controls.	<ul style="list-style-type: none"> <li>sn_grc.reader</li> <li>sn_grc.user</li> <li>sn_grc.manager</li> <li>sn_compliance.reader</li> <li>sn_compliance.user</li> </ul>

Role title [name]	Description	Contains roles
Compliance Administrator [sn_compliance.admin]	Contains the reader, user, manager, and admin roles in sn_grc scopes, and the reader, user, and manager roles in thePolicy and Compliance Management application. In addition to the inherited permissions, the compliance admin can delete authority documents, citations, policies, policy statements, and controls.	<ul style="list-style-type: none"> <li>• sn_grc.reader</li> <li>• sn_grc.user</li> <li>• sn_grc.manager</li> <li>• sn_grc.admin</li> <li>• sn_compliance.reader</li> <li>• sn_compliance.user</li> <li>• sn_compliance.manager</li> </ul>
Compliance Developer [sn_compliance.developer]	Contains the reader, user, manager, admin, and developer roles in sn_grc scopes, and the reader, user, manager, and admin roles in thePolicy and Compliance Management application. In addition to the inherited permissions, the compliance developer can create article templates and edit scripts.	<ul style="list-style-type: none"> <li>• sn_grc.reader</li> <li>• sn_grc.user</li> <li>• sn_grc.manager</li> <li>• sn_grc.admin</li> <li>• sn_grc.developer</li> <li>• sn_compliance.reader</li> <li>• sn_compliance.user</li> <li>• sn_compliance.manager</li> <li>• sn_compliance.admin</li> </ul>
Attestation Creator sn_compliance.attestation_creator	Role used for creating GRC attestation metric type	

## Script includes installed with Policy and Compliance Management

GRC: Policy and Compliance Management adds the following script includes.

Script include	Description
ComplianceAjax	AJAX utilities for compliance
ComplianceMigrationUtils	Utilities for migrating authority documents, citations, policies, controls/policy statements, and control test definitions from previous instances.
ComplianceUtils	Utilities for Policy and Compliance Management
ComplianceUtilsBase	Utilities for Policy and Compliance Management
ControlGeneratorStrategy	Creates controls for profile.
ControlGeneratorStrategyBase	Generates controls when relationships between profiles, profile types, policies, and policy statements are made.

## Client scripts installed with Policy and Compliance Management

GRC: Policy and Compliance Management adds the following client scripts.

Client script	Table	Description
Display incorrect answers onLoad	Assessment Metric [asmt_metric]	Show/hide the correct answer fields based on category (metric type), data type, and method.
Force positive weighting	Control [sn_compliance_control]	Enforces that the weighting field is greater than or equal to 0.
Populate fields from policy statement	Control [sn_compliance_control]	Populates the name, description, type, category, and classification from the policy statement.
Show/Hide incorrect answer on datatype	Assessment Metric [asmt_metric]	If the datatype is required, show the incorrect answer choices.
Show/Hide incorrect answer on method	Assessment Metric [asmt_metric]	If the method is script, show the incorrect answer choices.
Show/Hide incorrect answer on scored	Assessment Metric [asmt_metric]	If Scored is checked, show the incorrect answer choices.

## Business rules installed with Policy and Compliance Management

GRC: Policy and Compliance Management adds the following business rules.

Business rule	Tables	Description
Add processing document	Policy to Profile Type [sn_compliance_m2m_policy_profile_type]	
Add processing statement	Policy Statement to Profile Type [sn_compliance_m2m_statement_profile_type]	
Allow only one default	Article Template [sn_compliance_article_template]	Ensures that only one template record has the default check box checked.
Auto business rule for Assessments	Control [sn_compliance_control]	Automatically creates an Assessable Record when controls are created
Auto deletion rule for Assessments	Control [sn_compliance_control]	Automatically deletes the associated Assessable Record when a control is deleted
Cascade Changes	Policy Statement [sn_compliance_policy_statement]	Copies changes made to policy statement name, description, reference, category, type, and classification fields to the associated controls

Business rule	Tables	Description
Create issue for non-compliant control	Control [sn_compliance_control]	If no issues exist, creates an issue when a control status changes to non-compliant. Otherwise, a worknote is added to the existing issue.
Deactivate retired policy	Policy [sn_compliance_policy]	Sets the Active field to false when a policy state changes to Retired.
Enforce fields	Policy [sn_compliance_policy]	Ensures that the Valid to and Article template fields are populated before moving to the Awaiting Approval or Published states.
Enforce positive weighting	Control [sn_compliance_control]	Ensures that the weighting of a control is greater than or equal to 0.
Generate items	Policy Statement [sn_compliance_policy_statement]	
Issue close rollup response to control	Issue [sn_grc_issue]	Sets a control status to Compliant when all issues are closed.
Mark control as non-compliant	Issue [sn_grc_issue]	Sets a control status to non-compliant when a related issue is created.
Prevent adding inactive policy	Policy to Profile Type [sn_compliance_m2m_policy_profile]	Prevents relating inactive policies with profile types.
Prevent adding inactive policy statement	Policy Statement to Profile Type [sn_compliance_m2m_statement_profile_type]	Prevents relating inactive policy statements with profile types.
Prevent generation during retirement	Policy Statement to Profile Type [sn_compliance_m2m_statement_profile_type]	
Prevent generation during retirement	Policy to Profile Type [sn_compliance_m2m_policy_profile_type]	
Publish to KB	Policy [sn_compliance_policy]	Creates a knowledge article and publishes it to the default Knowledge Base once a policy state changes to Published
Retire KB Article	Policy [sn_compliance_policy]	Retires the associated knowledge article when a policy is retired or re-published.
Set active	Policy Statement [sn_compliance_policy_statement]	Sets a policy statement to be active if the policy statement Policy field is populated with an active policy.

Business rule	Tables	Description
Set Content	Policy Statement to Profile Type [sn_compliance_m2m_statement_profile_type]	Sets the Content field to the same value as the Policy statement field.
Set Document	Policy to Profile Type [sn_compliance_m2m_policy_profile]	Sets the Document field to the same value as the Policy field.
Start policy approval workflow	Policy [sn_compliance_policy]	Starts the approval workflow for a policy when it moves to the Awaiting Approval state.
Start policy review workflow	Policy [sn_compliance_policy]	Starts the review workflow for a policy when it moves to the Published state.
Update risks control failure factor	Control [sn_compliance_control]	Updates the control failure factor for associated risks when the controls Status field changes.

## Dependency modeling and mapping

An important aspect of risk and compliance management is understanding how various parts of the organization are related to each other. Doing so allows for a more comprehensive risk assessment process. Stakeholders can more easily discern how risks in different parts of the organization and at different levels of the organization impact each other.

### Dependency modeling

Dependency modeling is one of the activities required in order to ensure that an organization establishes a uniform definition of risk across the enterprise. The dependency model defines what relationships are allowed between different types of areas in the organization. This enables more effective risk normalization and aggregation by allowing stakeholders to more effectively compare and contrast risk appetite and exposure at various levels of the enterprise.

Creating a dependency model involves creating profile classes and defining how classes are structured with respect to each other using the Roll up to field.

### Dependency mapping

Once dependency modeling is complete, you can build out a dependency map to define how different parts of the organization are related to each other. For example, you could specify that certain projects and business services could affect the HR department, which would in turn affect the enterprise.

Defining the dependency map involves creating profiles, defining the profile class for each profile, then relating profiles to each other by specifying the upstream/downstream relationship.

## Compliance

The Compliance module contains compliance overview information, and lists of your authority documents and citations.

## Overview

The Compliance Overview is available to compliance administrators and compliance managers, providing an executive view into compliance requirements, overall compliance, and compliance breakdowns.

**Table 2: Compliance Overview reports in the base system**

Name	Visual	Description
Compliance Requirements	Donut chart	Select a wedge to focus on a specific compliance area.
Overall Compliance	Donut chart	Displays the overall compliance of all the control requirements in the system. Selecting a specific wedge in the previous widget brings that area into focus.
Profile	Drop down list	Select one or more profiles to view and compare their compliance across multiple items.
Control State	Check list	Select or clear check boxes to view filter reports by control state.
Compliance by Authority Document	Bar Chart	Compare level of compliance depending on the selected profile and/or authority document.
Compliance breakdown	Multi-level Pivot	View a breakdown of control compliance by related authority documents and policies.
Non Compliant Profiles	Column Chart	Count of non-compliant control requirements grouped by profile.

## Authority Documents

Authority documents define policies, risks, controls, audits, and other processes to ensure adherence to the authoritative content.

Each authority document is defined in a record and the related lists on that record contain the individual conditions of the authority document.

The relationships of these authority document related list items are visible in the GRC Workbench in the Policy and Compliance Management application.

## Citations

Citations contain the provisions of the authority document, which can be interrelated. Citations break down an authority document into manageable themes.

You can create citations or import them from UCF authority documents and then create any necessary relationships between the citations.

## Create a citation

Usually, authority documents, citations, and policy statements are downloaded from UCF. However, citations can be created manually from an authority document.

Role required: sn\_compliance\_admin or sn\_compliance\_manager

1. Navigate to Policy and Compliance Authority Documents .
2. Open an authority document.
3. In the Citations Related List, click New.
4. Fill in the fields on the form, as appropriate.

**Table 3: Citation**

Field	Description
Name*	User-defined name that identifies this citation.
Source	A non-editable field with the source of the policy. For example, if the statement is from the UCF import, the source is UCF.
Source ID	The unique identification number used by the source to catalog this authority document.
Reference	Content reference.
Type	Type of citation created. Optional field not used for any processing. Use the value in this field in reports or to query for records of a specific type. <ul style="list-style-type: none"> <li>• Core Topic</li> <li>• Process</li> <li>• Control Objective</li> <li>• Control</li> <li>• Supporting information</li> </ul>
Authority document	Name of the parent authority document for this citation. When you create citations from the authority document form, the system completes this field automatically.
Active	A policy is marked active if it is not in the Draft or Retired state.
Parent	References the parent content.
Description	Description of the citation.

## Relate a policy statement to a citation

A single policy statement can be mapped to many citations from different authority documents. This function allows you to test a policy statement once while complying with many different citations.

Role required: sn\_compliance\_admin or sn\_compliance\_manager

1. Navigate to Policy and Compliance Citations .
2. Open a citation.
3. In the Policy statements related list, click New.
4. Fill in the fields on the form, as appropriate.

**Table 4: Policy Statement**

Field	Description
Name	The name of the policy statement.
Source	A non-editable field with the source of the policy. For example, if the statement is from the UCF import, the source is UCF.
Reference	A unique numerical identifier.
Policy	The parent policy statement supported by this policy statement.
Parent	References the parent content.
Active	If the policy statement is not in the Draft or Retired states, a policy is marked active.
Source ID	The unique identification number used by the source to catalog this authority document.



Field	Description
Category	<p>Select from a list of options:</p> <ul style="list-style-type: none"><li>• Acquisition or sale of facilities, technology, and services</li><li>• Audits and risk management</li><li>• Compliance and Governance Manual of Style</li><li>• Human Resources management</li><li>• Leadership and high level objectives</li><li>• Monitoring and measurement</li><li>• Operational management</li><li>• Physical and environmental protection</li><li>• Privacy protection for information and data</li><li>• Records management</li><li>• System hardening through configuration management</li><li>• Systems continuity</li><li>• Systems design, build, and implementation</li><li>• Technical security</li><li>• Third Party and supply chain oversight</li><li>• Root</li><li>• Deprecated</li></ul>
Classification	<p>Select from a list of options:</p> <ul style="list-style-type: none"><li>• Preventive</li><li>• Corrective</li><li>• Detective</li><li>• IT Impact Zone</li></ul>

Field	Description
Type	Select from a list of options: <ul style="list-style-type: none"> <li>• Acquisition/Sale of Assets or Services</li> <li>• Actionable Reports or Measurements</li> <li>• Audits and Risk Management</li> <li>• Behavior</li> <li>• Business Processes</li> <li>• Communicate</li> <li>• Configuration</li> <li>• Data and Information Management</li> <li>• Duplicate</li> <li>• Establish Roles</li> <li>• Establish/Maintain Documentation</li> <li>• Human Resources Management</li> <li>• Investigate</li> <li>• IT Impact Zone</li> <li>• Log Management</li> <li>• Maintenance</li> <li>• Monitor and Evaluate Occurrences</li> <li>• Physical and Environmental Protection</li> <li>• Process or Activity</li> <li>• Records Management</li> <li>• Systems Continuity</li> <li>• Systems Design, Build, and Implementation</li> <li>• Technical Security</li> <li>• Testing</li> <li>• Training</li> </ul>
Description	Describe the policy statement and how it supports the goals of the organization.

5. Click Submit.

## Deactivate a citation

The Active option in a citation indicates whether the citation has been retired.

Role required: sn\_compliance.admin or sn\_compliance.manager

1. Navigate to Policy and Compliance Citations .
2. Open a citation.
3. In the citation, clear the check box marked Active.

## Create an authority document

Authority documents manage a process and citations are created within them to manage points of the process. For example, the process called Building Security contains a citation for Entry Control.

Role required: sn\_compliance\_admin or sn\_compliance\_manager

1. Navigate to Policy and Compliance Compliance Authority Documents .
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 5: Authority Document**

Field	Value
Name	Name of the document.
Number	Read-only field that is automatically populated with a unique identification number.
Source	A non-editable field with the source of the policy. For example, if the statement is from the UCF import, the source is UCF.
Source ID	The unique identification number used by the source to catalog this authority document.
Version	The unique version number used by the source to identify this authority document.
Common name	Abbreviated version of the Name field.
Category	Category for this authority document.
Type	The document type: <ul style="list-style-type: none"> <li>• Audit Guideline</li> <li>• Best Practice Guideline</li> <li>• Bill or Act</li> <li>• Contractual Obligation</li> <li>• International or National Standard</li> <li>• Not Set</li> <li>• Organizational Directive</li> <li>• Regulation of Statute</li> <li>• Safe Harbor</li> <li>• Self-Regulatory Body Requirement</li> <li>• Vendor Documentation</li> </ul>
Valid From	The date and time for which the policy becomes valid.
Valid To	The date and time for which the policy is no longer valid.
Url	The URL of the stored authority document.
Description	More information about the authority document.

4. Right-click in the header bar and select Save from the context menu.  
The authority document is created and all related lists are visible.

Create a citation from the Authority document related list.

## Deactivate an authority document

The Active option in an authority document indicates whether the authority documents has been retired.

Role required: sn\_compliance.admin or sn\_compliance.manager

1. Navigate to Policy and Compliance Compliance Authority Documents .
2. Open an authority document.
3. In the authority document, clear the check box marked Active.

## Policies and procedures

The Policies and Procedures module contains overview and detailed information related to policy approvals, policies, and policy statements.

### Overview

The Policies and Procedures Overview is contained in the Policies and procedures module and provides an executive view into compliance requirements, overall compliance, and compliance breakdowns so areas of concern can be identified quickly. Users with the Compliance Administrator and Compliance Manager roles view the Policies and Procedures Overview.

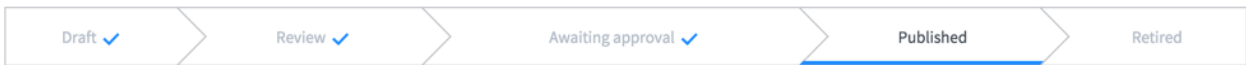
**Table 6: Policies and Procedures Overview reports in the base system**

Name	Visual	Description
Control compliance	Donut chart	Displays the overall compliance of all the controls in the system.
Control details	Donut chart	Displays a breakdown of controls, grouped by owner, category, or type.
Control Overview	Column Chart	Displays the total number of controls related to each policy. The chart is stacked to display overall control compliance status for each policy.
Control Issues by Policy (Opened Date)	Line Chart	Displays the number of control issues opened each week, grouped by policy.
Policy Exceptions	List	Displays a list of control issues that have been closed with a response value of accept, meaning the issue was not remediated.

Name	Visual	Description
Total Policy Statements by Policy	Bar graph	Displays a count of the overall number of policy statements in each policy. The chart is stacked to display policy statements by type.

## My Policy Approvals

My Policy Approvals is contained in the Policy and Compliance module and contains all policies requiring your approval. Policies go through an approval process. Compliance managers set the length of time that policies are valid, ensuring that the team reviews the policy often to affirm its validity. Policies have a type, such as a policy, procedure, standard, plan, checklist, framework, or template.



## Policies

Compliance managers catalog and publish internal policies that define a set of business processes, procedures, and or standards.

## Policy Statements

Compliance managers catalog the policy statements and generate controls from those policy statements.

Policy statements only reference a single policy, although they can cover multiple citations from different authority documents. They can be organized into Classification, Category, and Type.

---

**Note:** UCF refers to policy statements as Controls. When UCF is data is imported, controls are imported into the policy statements table.

---

## Create a policy

A policy is a document which defines an internal practice that processes must follow. Policies are defined as policies, procedures, standards, plans, checklists, frameworks, and templates.

Role required: sn\_compliance\_admin or sn\_compliance\_manager

1. Navigate to Policy and Compliance Policies and Procedures Policies .
2. Click New.
3. Fill in the fields on the form, as appropriate.

Table 7: Policy

Field	Description
Name	The name of the policy.
Type	Select from a list of options: <ul style="list-style-type: none"> <li>• Policy</li> <li>• Procedure</li> <li>• Standard</li> <li>• Plan</li> <li>• Checklist</li> <li>• Framework</li> <li>• Template</li> </ul>
Owning Group	Group that owns the policy.
Owner	User that owns the policy.
State	The policy state is a read-only field. Possible choices are: <ul style="list-style-type: none"> <li>• Draft In this state, all compliance users can modify the policy and policy statements. All compliance users can click Ready for Review at the bottom of the form, which sets the state to Review.</li> <li>• Review In this state, the owner, owning group, and reviewers can modify the policy and policy statements. The owner, owning group, and reviewers click Request approval, starting the workflow by sending approvals to the users in the Approvers list. The owner, owning group, and reviewers move the policy back to Draft, by clicking Back to draft, as well.</li> <li>• Awaiting approval In this state, the policy and policy statements are read- only for all. Approvers can approve the policy by updating the approval state in the Approvals Related List on the policy form, or by viewing My Approvals. If the policy is approved, the policy goes to the Published state. Otherwise, it goes back to the Review state.</li> <li>• Published In this state, the policy and policy statements are read-only for all. Admins can click Retire which sets the state of the policy to Retired</li> <li>• Retired In this state, the policy is read-only for all.</li> </ul>
Valid From	The date and time for which the policy becomes valid.

Field	Description
Valid To	The date and time for which the policy is no longer valid.
Approvers	Select the users you want to be included in the approval process.
Reviewers	Select the users you want to be included in the review process.
Description	A general description of the policy.
Policy text	A detailed description of the policy.
Article template	The article template to use for the publication of this policy.
KB article	The KB article number and link where the policy is published.

4. Continue with one of the following options.

Option	Action
<b>To save and submit the policy</b>	<ul style="list-style-type: none"> <li>Click Submit.</li> </ul>
<b>To mark the policy ready for review</b>	<ul style="list-style-type: none"> <li>Click Ready for review.</li> </ul>

## Review a policy

It is important that the right people in your organization are involved in the review of policies.

Role required: sn\_compliance\_admin or sn\_compliance\_manager

- Navigate to Policy and Compliance Policies and Procedures Policies .
- Open the Policy record.
- Review the policy details, making updates as necessary.
- Continue with one of the following actions:

Option	Action
<b>To move the policy back into draft</b>	<ul style="list-style-type: none"> <li>Click Back to draft.</li> </ul>
<b>To request approval for the policy</b>	<ul style="list-style-type: none"> <li>Click Request approval.</li> </ul>

## Approve a policy

When a policy is approved, it is automatically published.

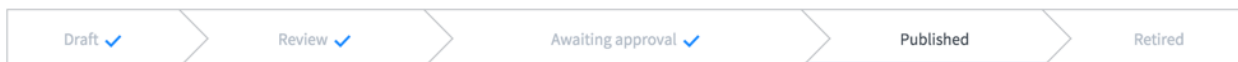
Role required: sn\_compliance\_admin or sn\_compliance\_manager

- Navigate to Policy and Compliance Policies and Procedures Policies .
- Open the policy record.
- Review the policy details, making updates as necessary.

## 4. Click Approve.

## Policy approval and publishing

Policies are part of a strict approval process to ensure compliance and to reduce exposure to risk. Publishing a policy is automatically incorporated in the approval process.



**Table 8: Policy approval states**

State	Description
Draft	All policies start in Draft state. In this stage, all compliance users can modify the policy and policy statements.
Review	The owner, owning group, and reviewers can modify the policy and policy statements and send it on to the next state.
Awaiting Approval	The policy is read only in this state. Approved policies move forward to the Published state. Unapproved policies move back to Review. If no approvers are identified on the policy form, the state is skipped and published without an approval.
Published	Approved policies are automatically published to a template-defined KB. Once a policy is published, it remains in a read-only state. The Valid to field on the policy form defines how long the policy is valid. When a policy is no longer valid, it is automatically sent back to Draft state.  When a policy reaches the end of the Review state and is Approved for publishing, it is automatically published to the GRC knowledge base (as defined in the Policy and Compliance Administration Properties). The article template field on the policy form defines the style of the published policy.
Retired	The KB article is removed when a policy is put into a Retired state.

## Retire a policy

Retiring a policy is part of the policy management process. It can be retired any time after being approved and published to the KB.



Role required: sn\_compliance\_admin or sn\_compliance\_manager

1. Navigate to Policy and Compliance Policies .
2. Open the Policy record.
3. In the top right corner, click Retire.

This option is available only for policies in a published state.

## Create a policy statement

A policy statement is an objective, direction, or standard that acts as guidance for company interactions and operations. Policy statements can be categorized, classified, and related to policies.

Role required: sn\_compliance.admin or sn\_compliance.manager

1. Navigate to Policy and Compliance Policy Statements .
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 9: Policy Statement**

Field	Description
Name*	The name of the policy statement.
Source	A non-editable field with the source of the policy. For example, if the statement is from the UCF import, the source is UCF.
Source ID	The unique identification number used by the source to catalog this authority document.
Reference	A unique numerical identifier
Policy	The parent policy containing the policy statement. If you create a policy statement from within a policy, this field is automatically filled.
Parent	The parent policy statement.
Active	A policy is marked active if it is not in the Draft or Retired state.
Creates controls automatically	<p>Check box indicating that controls are automatically created from the policy statement.</p> <p><b>Note:</b> Select this option if the policy statement can also serve as the control.</p>

Field	Description
Category	<p>Select from a list of options:</p> <ul style="list-style-type: none"><li>• Acquisition or sale of facilities, technology, and services</li><li>• Audits and risk management</li><li>• Compliance and Governance Manual of Style</li><li>• Human Resources management</li><li>• Leadership and high level objectives</li><li>• Monitoring and measurement</li><li>• Operational management</li><li>• Physical and environmental protection</li><li>• Privacy protection for information and data</li><li>• Records management</li><li>• System hardening through configuration management</li><li>• Systems continuity</li><li>• Systems design, build, and implementation</li><li>• Technical security</li><li>• Third Party and supply chain oversight</li><li>• Root</li><li>• Deprecated</li></ul>
Classification	<p>Select from a list of options:</p> <ul style="list-style-type: none"><li>• Preventive</li><li>• Corrective</li><li>• Detective</li></ul>

Field	Description
Type	Select from a list of options: <ul style="list-style-type: none"> <li>• Acquisition/Sale of Assets or Services</li> <li>• Actionable Reports or Measurements</li> <li>• Audits and Risk Management</li> <li>• Behavior</li> <li>• Business Processes</li> <li>• Communicate</li> <li>• Configuration</li> <li>• Data and Information Management</li> <li>• Duplicate</li> <li>• Establish Roles</li> <li>• Establish/Maintain Documentation</li> <li>• Human Resources Management</li> <li>• Investigate</li> <li>• IT Impact Zone</li> <li>• Log Management</li> <li>• Maintenance</li> <li>• Monitor and Evaluate Occurrences</li> <li>• Physical and Environmental Protection</li> <li>• Process or Activity</li> <li>• Records Management</li> <li>• Systems Continuity</li> <li>• Systems Design, Build, and Implementation</li> <li>• Technical Security</li> <li>• Testing</li> <li>• Training</li> </ul>
Attestation	Select from a list of options. <ul style="list-style-type: none"> <li>• GRC Attestation is chosen by default</li> <li>• <b>Note:</b> If the user changes the control's attestation, the related policy statement's attestation type is changed also.</li> </ul>
Description	Description of the policy statement.

4. Click Submit.

The policy statement is created and all related lists are visible.

- A control is created for every policy statement when a policy is associated with a profile.
- The control attributes default to the same attributes as the related policy statement.

## Relate a policy statement to a policy

Policy statements can be associated to a policy individually by choosing the policy in the document field on the policy statement, or by editing the policy statements related list.

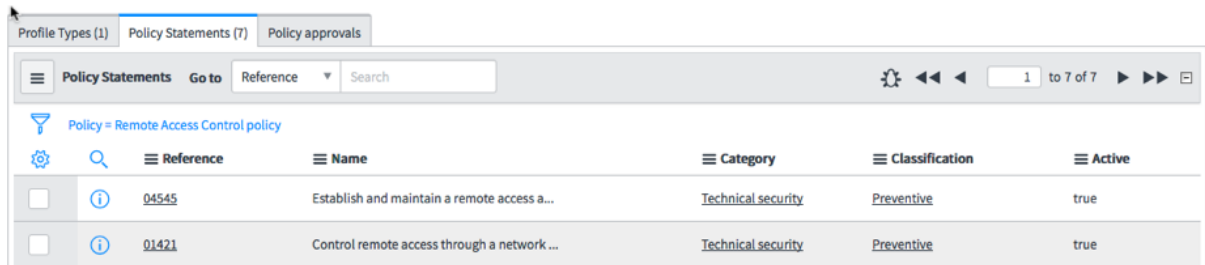
Role required: sn\_compliance.admin or sn\_compliance.manager

1. Navigate to Policy and Compliance Policies and Procedures Policies .
2. Open the policy record.
3. Click Edit in the Policy Statements related list.

The slushbucket contains active policy statements with no associated policy selected.

4. Select the policy statements.
5. Click Save.

Those policy statements are listed in the Policy Statement related list.



## Relate a policy statement to a citation

A single policy statement can be mapped to many citations from different authority documents. This function allows you to test a policy statement once while complying with many different citations.

Role required: sn\_compliance\_admin or sn\_compliance\_manager

1. Navigate to Policy and Compliance Compliance Citations .
2. Open a citation.
3. In the Policy statements related list, click New.
4. Fill in the fields on the form, as appropriate.

**Table 10: Policy Statement**

Field	Description
Name	The name of the policy statement.
Source	A non-editable field with the source of the policy. For example, if the statement is from the UCF import, the source is UCF.

Field	Description
Reference	A unique numerical identifier.
Policy	The parent policy statement supported by this policy statement.
Parent	References the parent content.
Active	If the policy statement is not in the Draft or Retired states, a policy is marked active.
Source ID	The unique identification number used by the source to catalog this authority document.
Category	<p>Select from a list of options:</p> <ul style="list-style-type: none"> <li>• Acquisition or sale of facilities, technology, and services</li> <li>• Audits and risk management</li> <li>• Compliance and Governance Manual of Style</li> <li>• Human Resources management</li> <li>• Leadership and high level objectives</li> <li>• Monitoring and measurement</li> <li>• Operational management</li> <li>• Physical and environmental protection</li> <li>• Privacy protection for information and data</li> <li>• Records management</li> <li>• System hardening through configuration management</li> <li>• Systems continuity</li> <li>• Systems design, build, and implementation</li> <li>• Technical security</li> <li>• Third Party and supply chain oversight</li> <li>• Root</li> <li>• Deprecated</li> </ul>
Classification	<p>Select from a list of options:</p> <ul style="list-style-type: none"> <li>• Preventive</li> <li>• Corrective</li> <li>• Detective</li> <li>• IT Impact Zone</li> </ul>

Field	Description
Type	Select from a list of options: <ul style="list-style-type: none"> <li>• Acquisition/Sale of Assets or Services</li> <li>• Actionable Reports or Measurements</li> <li>• Audits and Risk Management</li> <li>• Behavior</li> <li>• Business Processes</li> <li>• Communicate</li> <li>• Configuration</li> <li>• Data and Information Management</li> <li>• Duplicate</li> <li>• Establish Roles</li> <li>• Establish/Maintain Documentation</li> <li>• Human Resources Management</li> <li>• Investigate</li> <li>• IT Impact Zone</li> <li>• Log Management</li> <li>• Maintenance</li> <li>• Monitor and Evaluate Occurrences</li> <li>• Physical and Environmental Protection</li> <li>• Process or Activity</li> <li>• Records Management</li> <li>• Systems Continuity</li> <li>• Systems Design, Build, and Implementation</li> <li>• Technical Security</li> <li>• Testing</li> <li>• Training</li> </ul>
Description	Describe the policy statement and how it supports the goals of the organization.

5. Click Submit.

## Deactivate a policy statement

Deactivate policy statements that are no longer relevant to their citation or policy statement.

Role required: sn\_compliance\_admin or sn\_compliance\_manager

1. Navigate to Policy and Compliance Policies and Procedures Policy Statements .
2. Open a policy statement.
3. In the policy statement, clear the check box marked Active.
4. Click Update.

## GRC profile scoping

The Scoping module contains profiles and profile types for use in all GRC-related applications. They can be created for any record on any table.

The GRC: Profile plugin contains the Scoping module and is not visible to customers and requires activation of the Policy and Compliance Management plugin, the Risk Management plugin, or the Audit Management plugin.

Only one profile can exist for a record. That profile, however, can belong to many profile types. Profile types and profiles are used differently depending on the application:

- Risk managers use profile types and profiles to monitor risk exposure and perform risk assessments.
- Policy and compliance managers use profile types and profiles to create a system of internal controls and monitor compliance.

### Profiles

Profiles are the records that aggregate GRC information related to a specific item. Each profile is associated with a single record from any table in the application. Profiles cannot be created for items that do not have a record in a table in the platform.

### Profile Classes

Profile classes allow GRC managers to separate profiles for better distinction. For example, Business Service Profiles, Department Profiles, Business Unit Profiles, and the like.

### Profile Types

Profiles types are dynamic categories containing one or more profiles. Business logic automates the process of creating and categorizing any profiles in the system that meet the profile type conditions. Profile types are assigned to policy statements, which generate controls for every profile listed in the profile type.

## Create and edit a profile type

Administrators or managers in any of the GRC-related applications, create profiles types from which profiles are generated.

Role required: sn\_compliance.admin or sn\_compliance.manager, sn\_risk.admin or sn\_risk.manager, sn\_audit.admin or sn\_audit.manager

1. Navigate to one of the following locations:
  - Audit Scoping Profile Types .
  - Policy and Compliance Scoping Profile Types .
  - Risk Scoping Profile Types .

2. Do one of the following actions:

Option	Description
<b>To create a new profile type</b>	Click New.
<b>To edit a profile type</b>	Open the profile type.

3. Fill in the fields on the form, as appropriate.

Table 11: Profile type

Name	Description
Name*	The name of the profile type.
Description	An explanation of the profile type with any additional information about the profile type that a user will find helpful.
Table*	The table from which the profile type conditions identify the records to create profiles.
Condition	Filter conditions to restrict which profiles belong to a specific profile type.
Use owner field	Select the check box to indicate that a default owner field should be used when generating new profiles.
Default owner	The field on the table specifying the person who owns any new profiles generated from the profile type.
Default profile class	<p>Set the default profile class.</p> <p>Generated profiles copy this default profile class under the following conditions:</p> <ul style="list-style-type: none"> <li>when the profile's class is empty and it's associated to a profile type that has a default profile class</li> <li>when a profile is created under a profile type that has a default profile class</li> </ul> <p>The existing profile's class is updated under the following conditions:</p> <ul style="list-style-type: none"> <li>The profile type's table changes</li> <li>The profile type's condition changes</li> <li>The profile type's active field is ik;8,'</li> <li>The profile type's default profile class changes</li> </ul>

---

**Note:** \* indicates a mandatory field.

---

4. Click Submit.

## Generate a profile from a profile type

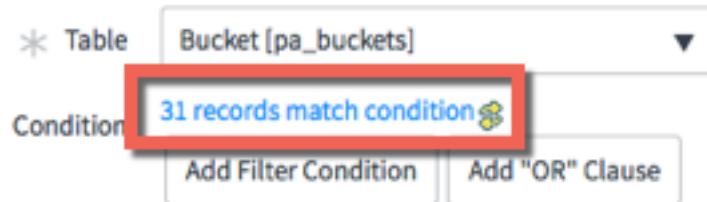
Profiles are generated automatically from profile types in any of the GRC-related applications.



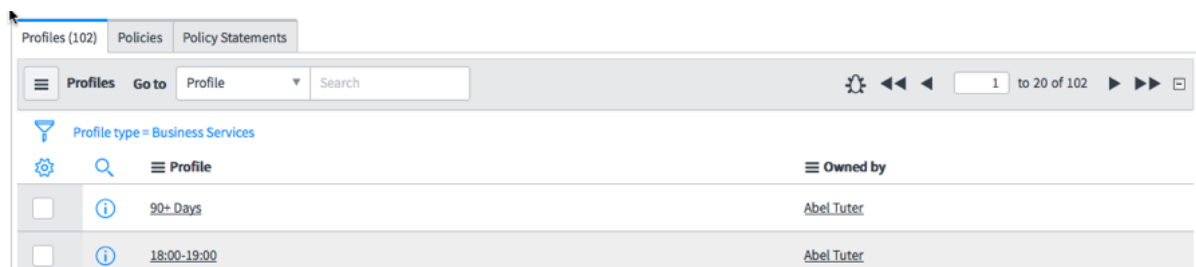
Role required: sn\_compliance.admin or sn\_compliance.manager, sn\_risk.admin or sn\_risk.manager, sn\_audit.admin or sn\_audit.manager

1. Navigate to one of the following locations:
  - Audit Scoping Profile Types
  - Policy and Compliance Scoping Profile Types
  - Risk Scoping Profile Types
2. Open the Profile Type record.
3. Add or modify any conditions, as necessary.

Changing the Table, changes the number of records matching the condition.



4. Assign the Owner field.
5. Click Update.  
A profile is generated for every record that matches the filter condition.



## Deactivate a profile

When a profile is deactivated, all the controls related to that profile are retired, and the indicators and test plans associated to those controls are marked in-active.

Role required: grc\_manager

The owner of the profile can edit the profile record and deactivate it.

1. Navigate to one of the following locations:
  - Audit Scoping All Profiles
  - Policy and Compliance Scoping All Profiles
  - Risk Scoping All Profiles

2. Open the profile record.
  - If the Active check box is selected, then the profile is active.
  - If the Active check box is not selected, then the profile is inactive.
3. Click Update.
  - All associated controls change to the retired state.
  - All the indicators and test plans associated with the retired control are marked in-active.

## Reactivate a profile

When a profile is reactivated, associated controls and risks return to the draft state and the indicators and test plans return to active.

Role required: grc\_manager

The owner of the profile can edit the profile record and reactivate it.

1. Navigate to one of the following locations:
  - Audit Scoping All Profiles
  - Policy and Compliance Scoping All Profiles
  - Risk Scoping All Profiles
2. Open the profile record.
3. In the profile, select the check box marked Active.
4. Click Update.
 

All associated controls, risks, indicators, and test plans are also re-activated or retired.

## Create a profile class

GRC managers create profile classes representing the types of things that will be part of the dependency model. Reports can be filtered to define relationships between the different profile classes. A profile class defines what a profile actually is. It differs from a profile type (for example, Business Services and Critical Business Services), in that a profile can belong to many profile types but a profile can have only one profile class (for example, Business Service).

Role required: sn\_grc.manager

1. Navigate to one of the following locations:
  - Audit Scoping Profile Classes
  - Policy and Compliance Scoping Profile Classes
  - Risk Scoping Profile Classes
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 12: Authority Document**

Field	Value
Name	Name of the profile class.

Field	Value
Roll up to	Select dependencies to other profiles. Useful for reporting how your lower-level operational risks impact corporate-level risks.
Is Root	Select the check box to indicate that this is the highest level class.  <b>Note:</b> Only one root class is allowed and it cannot roll up to another class.

4. Click Submit.

## Relate profiles to each other

Create relationships between profiles to build out the dependency map and better understand how risks affect each other and how they affect the enterprise.

Role required: sn\_grc.manager

1. Navigate using any of these options.
  - Audit Scoping All Profiles
  - Policy and Compliance Scoping All Profiles
  - Risk Scoping All Profiles
2. Open the profile record.
3. Perform one of the following actions:

Option	Description
<b>To specify that the current profile is downstream of another profile</b>	Click the Add button in the Upstream profiles related list.
<b>To specify that the current profile is upstream of another profile</b>	Click the Add button in the Upstream profiles related list.

4. Select the desired profiles to relate the current profile to and click Create Relationship.

The profiles displayed after clicking the Add button on the Upstream profiles or Downstream profiles related lists are limited based on the current profile's class and the defined dependency model.

**Note:** If there are no eligible profiles which can be related to the current profile, then the Add button is not displayed on the Upstream profiles or Downstream profiles related lists.

## Set a profile's class

Set the profile class for a profile to relate the profile to others.

Role required: sn\_grc.manager

1. Navigate using any of the following options.
  - Audit Scoping All Profiles
  - Policy and Compliance Scoping All Profiles

- Risk Scoping All Profiles
2. Open the profile record.
  3. Set the class field to the desired class.
  4. Click Update.

## Assign profiles to classes

GRC managers assign profiles to classes for the filtering of reports and to define relationships between the different classes of business services.

Role required: sn\_compliance.manager

1. Navigate to one of the following locations:
  - Audit Scoping All Profiles
  - Policy and Compliance Scoping All Profiles
  - Risk Scoping All Profiles
2. Open the profile record.
3. Assign the Class.
4. Click Update.

## Use UCF Common Controls Hub to manage compliance frameworks

Compliance administrators can download content from Network Frontiers Unified Compliance Framework (UCF) for use as GRC authority documents, citations, controls, and policy statements. The documents can be updated on pre-defined intervals.

Users must have a UCF Common Controls Hub account to create shared lists and import them into the ServiceNow® instance.

For more information on Unified Compliance Framework (UCF), see <https://www.unifiedcompliance.com>.



---

**Warning:** All data imported from UCF Authority Documents is read-only and must be protected. Do not customize the authority documents, citations, or policy statements on any UCF fields transformed into GRC tables.

---

### Getting Started with the UCF Common Controls Hub

Network Frontiers released a new method for allowing authenticated users to download content from the UCF Common Controls Hub (CCH) website. Users require a separate subscription to the Network Frontiers Unified Compliance Framework Common Controls Hub (UCF-CCH) to download UCF content.

For customers whose GRC entitlement date is before December 1, 2016, you are entitled to a free UCF CCH account for the period of December 1, 2016 through November 30, 2018.

For customers on Helsinki (Patch 7 and above), or Istanbul, and whose GRC entitlement date is December 1, 2016 or after, you must contact [UCF-Common Control Hub](#) to arrange for a subscription, if your organization plans on using Unified Controls Compliance as the provider of your controls library. For more information about establishing a UCF CCH account, see [Unified Compliance Framework](#).

**Note:** A subscription to UCF-CCH is not required for using the GRC Policy & Compliance application.

**Table 13:**

If your organization's GRC entitlement date is	Tasks
BEFORE December 1, 2016	<ol style="list-style-type: none"> <li>1. <a href="#">Activate Compliance UCF.</a></li> <li>2. <a href="#">Create HI Request for GRC subscription validation free UCF-CCH account</a> on page 39.</li> <li>3. <a href="#">Configure the UCF integration</a> on page 43.</li> <li>4. <a href="#">Download a UCF shared list</a> on page 45.</li> </ol>
AFTER December 1, 2016	<ol style="list-style-type: none"> <li>1. Sign up for a <a href="#">UCF CCH</a> account and customize your basic subscription to include API Access.</li> <li>2. <a href="#">Activate Compliance UCF.</a></li> <li>3. <a href="#">Create HI Request for UCF-CCH account integration information</a> on page 41.</li> <li>4. <a href="#">Configure the UCF integration</a> on page 43.</li> <li>5. <a href="#">Download a UCF shared list</a> on page 45.</li> </ol>

### Authority document and shared list imports

Every authority document already imported into the ServiceNow® instance must be in any shared list you wish to import from the UCF CCH. This prevents inconsistencies between what is in the UCF CCH (which may have changed) and what you've already imported.

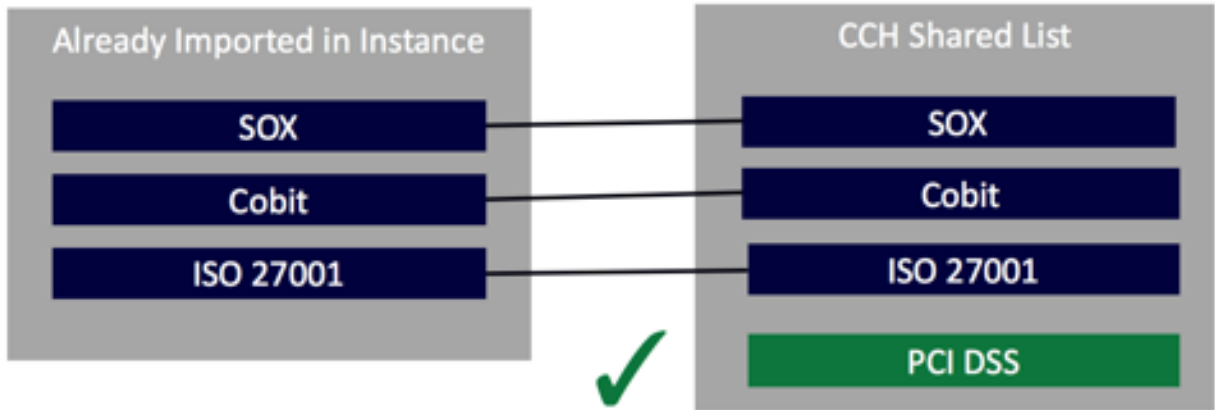


Figure 2: Shared list import successful



Figure 3: Shared list import unsuccessful

An error is rendered since SOX is not being reimported within this Shared List.

### UCF and GRC terminology differences

Authority documents in the UCF content are organized and mapped to their proper citations, which in turn are mapped to a common set of controls. The terminology between UCF and the GRC applications differ slightly as explained in the following table.

Table 14: Terminology differences

UCF	GRC application
Authority Document	Authority Document
Citation	Citation
Control	Policy Statement

## Activate Compliance UCF

The GRC: UCF Import (com.snc.ucf\_import\_add\_on) plugin was deprecated and replaced by the new GRC: Compliance UCF (com.sn\_comp\_ucf) plugin, as an add-on to the GRC: Policy and Compliance Management application. This plugin is required to import content from the UCF-CCH.

Role required: admin

This plugin includes demo data and activates related plugins if they are not already active.

1. Navigate to System Definition Plugins .
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

If the plugin has optional features that are not functional because other plugins are inactive, those plugins are listed. A warning states that some files are not installed. If you want the optional features to be installed, cancel this activation, activate the necessary plugins, and then return to activating the plugin.

4. If available, select the Load demo data check box.

Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.

5. Click Activate.

For customers whose GRC entitlement date is before December 1, 2016, a free UCF CCH account is included for the period of December 1, 2016 through November 30, 2018. See [Create HI Request for GRC subscription validation free UCF-CCH account](#) on page 39.

For customers on Helsinki (Patch 7 and above), or Istanbul, and whose GRC entitlement date is December 1, 2016 or after, you must contact [UCF-Common Control Hub](#) to arrange for a basic account subscription with API access.

---

**Note:** API access is required to download UCF content from the UCF-CCH.

---

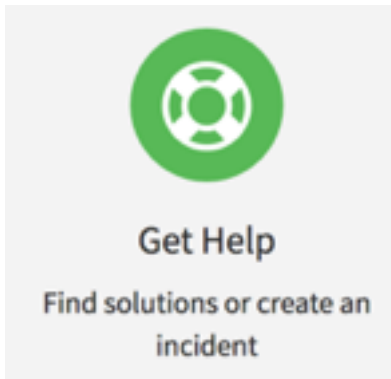
For more information about establishing a UCF CCH account, see [Unified Compliance Framework](#).

## Create HI Request for GRC subscription validation free UCF-CCH account

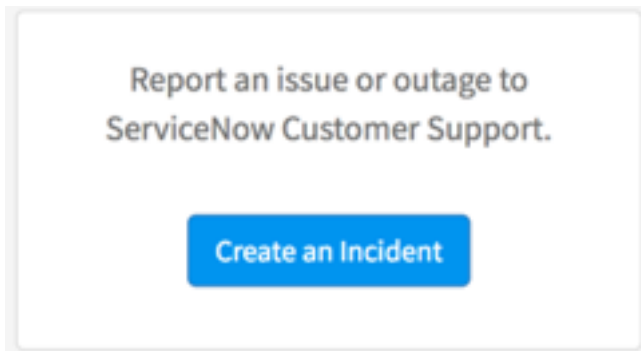
For customers whose GRC entitlement date is before December 1, 2016, a free UCF CCH account is included for the period of December 1, 2016 through November 30, 2018.

Role required: admin

1. After activating the Compliance UCF plugin, sign in to the [Hi Service Portal](#).
2. Click Get Help.



3. Click Create an Incident.



4. Select Issue Type Request.

Report an Issue

Select Issue Type **(Required)**

- Question  
If you want more information on using or administering your ServiceNow instance.
- Request  
If you need ServiceNow to perform a task in your instance not available in the [Service Catalog](#).
- Something is broken  
If you experience unexpected behaviour in your instance.
- Performance issue  
If you experience slowness with your instance.
- Outage  
If you cannot access or use your instance.



5. Select Category Hi Administration.
6. Describe the issue and provide the following information:
  - Enter "I have activated the new GRC: Compliance UCF (com.sn\_comp\_ucf) plugin. I am requesting that you validate my subscription and open a UCF CCH account on my behalf".
  - Include your company name and company account number.
  - Include the requester's name, business email address and phone number.

---

**Note:** By providing your company and requester contact information, you authorize ServiceNow® customer service to contact and share that information with Network Frontiers, a third party, in order to complete your UCF CCH account enrollment.

---

7. Attach screen shots, logs, etc., as necessary.
8. Select affected instances. Enter your company's GRC instance.
9. What is the business impact? Select your answer.
10. How many users does this affect? Select your answer.
11. When did you experience this issue? Select today's date.
12. Click Report the issue.  
ServiceNow® HI customer support initiates the UCF-CCH account creation and enrollment process and will contact the requester when the process is complete.

[Configure the UCF integration](#) on page 43

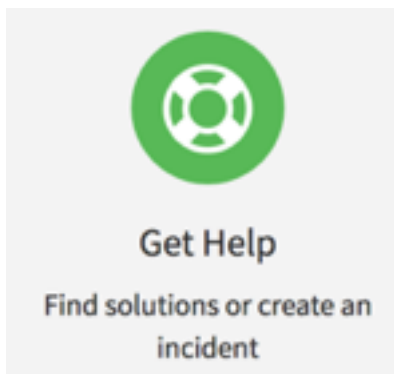
## Create HI Request for UCF-CCH account integration information

For customers on Helsinki (Patch 7 and above), or Istanbul, and whose GRC effective contract date is December 1, 2016 or after, you must contact [UCF-Common Control Hub](#) to arrange for a subscription, if your organization plans on using Unified Controls Compliance as the provider of your controls library. For more information about establishing a UCF CCH account, see [Unified Compliance Framework](#).

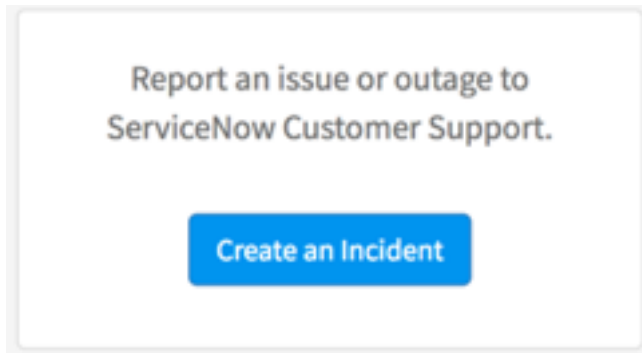
Sign up for a [UCF CCH](#) account and customize your basic subscription to include API Access.

Role required: admin

1. After activating the Compliance UCF plugin, sign in to the [Hi Service Portal](#).
2. Click Get Help.



3. Click Create an Incident.



4. Select Issue Type Request.

A screenshot of the "Report an Issue" form in ServiceNow. The form title is "Report an Issue". Below the title is a section titled "Select Issue Type (Required)". This section contains five radio button options, each with a brief description:

- Question**  
If you want more information on using or administering your ServiceNow instance.
- Request**  
If you need ServiceNow to perform a task in your instance not available in the [Service Catalog](#).
- Something is broken**  
If you experience unexpected behaviour in your instance.
- Performance issue**  
If you experience slowness with your instance.
- Outage**  
If you cannot access or use your instance.

5. Select Category Hi Administration.

6. Describe the issue and provide the following information:

- Enter "I have activated the new GRC: Compliance UCF (com.sn\_comp\_ucf) plugin. I have already subscribed to the UCF CCH. I am requesting that you provide me with the necessary OAuth information to complete the integration."
- Include your company name and company account number.
- Include the requester's name, business email address and phone number.

---

**Note:** By providing your company and requester contact information, you authorize ServiceNow® customer service to contact and share that information with Network Frontiers, a third party, in order to complete your UCF CCH account enrollment.

---

7. Attach screen shots, logs, etc., as necessary.
8. Select affected instances. Enter your company's GRC instance.
9. What is the business impact? Select your answer.
10. How many users does this affect? Select your answer.
11. When did you experience this issue? Select today's date.
12. Click Report the issue.

ServiceNow® HI customer support initiates the OAuth integration process and will contact the requester with the integration information.

[Configure the UCF integration](#) on page 43

## Configure the UCF integration

After ServiceNow® HI customer support provides you the UCF-CCH account integration information the OAuth integration process and will contact the requester with the integration information. After Create HI Request for UCF-CCH account integration information The UCF integration is an OAuth-based integration requiring a user's CCH Client ID and Client Secret.

Role required: sn\_comp\_ucf.admin and oauth\_admin

---

**Note:** Only the UCF Oauth administrator has access to the system Oauth tables. The user must give the UCF Oauth administrator role to the GRC UCF administrator, so the UCF administrator can set up UCF configuration page.

---

UCF integration requires that GRC is configured and users must be a Common Controls Hub administrator. The UCF integration is an OAuth based integration requiring a user's CCH Client ID and Client Secret.

The configuration page for the global domain is loaded by default. If you are using Domain Separation, delete the default configuration page, and create one specific to your domain.

1. Navigate to Policy and Compliance Administration Unified Compliance Integration .
2. Click the UCF configuration.
3. Fill in the fields on the form, as appropriate.

**Table 15: UCF Configuration**

Field	Description
Shared List	The shared list to be imported.
Client ID	<p>The UCF OAuth Client ID, provided by ServiceNow® HI customer support. See <a href="#">Getting Started with the UCF Common Controls Hub</a> on page 36 for information.</p> <hr/> <p><b>Note:</b> Configuration information is specific to the ServiceNow® instance. Be sure to enter accurate information for any test, development, or production instances you are using. Do not include spaces in the entry.</p> <hr/>

Field	Description
Client Secret	<p>The UCF OAuth Client Secret, provided by ServiceNow® HI customer support. See <a href="#">Getting Started with the UCF Common Controls Hub</a> on page 36 for information.</p> <hr/> <p><b>Note:</b> Configuration information is specific to the ServiceNow® instance. Be sure to enter accurate information for any test, development, or production instances you are using. Do not include spaces in the entry.</p> <hr/>
Oauth2 Profile	<p>The OAuth2 profile to use for downloading. The default is the United Compliance Framework Default Profile that is installed with the UCF plugin. This field does not typically need to be changed .</p>
Redirect URL	<p>Enter the Redirect URL, provided by ServiceNow® HI customer support. For example, <a href="https://mycompany.service-now.com/oauth_redirect.do">https://mycompany.service-now.com/oauth_redirect.do</a></p> <p>See <a href="#">Getting Started with the UCF Common Controls Hub</a> on page 36 for information.</p> <hr/> <p><b>Note:</b> Configuration information is specific to the ServiceNow® instance. Be sure to enter accurate information for any test, development, or production instances you are using. Do not include spaces in the entry.</p> <hr/>

4. Right-click the form header and click Save.
5. In the UCF Integration dialog that appears, click Request New Token.  
When configuring the UCF instance for the first time, a user with an UCF administrator account should request the new token.
6. Enter your Common Controls Hub credentials and log in.  
The first time the UCF administrator logs into UCF, a n application authorization message displays, click Authorize.
7. Select a shared list and click Save Configuration.

If UCF introduces new fields and content, administrators can use staging tables and transform maps to accommodate those changes to UCF data formats. This is an advanced configuration and not required. The following import sets and tables can be configured to customize the UCF download logic.

**Table 16: Staging table [extends from import set row table: import\_set\_row] used for UCF integration**

Staging table	Description
UCF Authority Document [sn_comp_ucf_authority_document]	The UCF Authority Document staging table is used to store authority documents that are downloaded from the UCF Common Controls Hub
UCF Citation [sn_comp_ucf_citation]	The UCF Citation staging table is used to store citations that are downloaded from the UCF Common Controls Hub
UCF Control [sn_comp_ucf_control]	The UCF Control staging table is used to store controls that are downloaded from the UCF Common Controls Hub
UCF Citation to Control [sn_comp_ucf_m2m_control_citation]	The UCF Citation to Control staging table is used to store citation to controls that are downloaded from the UCF Common Controls Hub

**Table 17: Transform maps used for UCF integration**

Transform maps	Description
Default Authority document transform	Transforms data from the UCF Authority document staging table into the Authority Document table
Default Citation Transform	Transforms data from the UCF Citation staging table into the Citation table
Default Control transform	Transforms data from the UCF Control staging table into the Policy Statement table
Control to Citation transform map	Transforms data from the UCF Citation to Control table into the Policy Statement to Citation table

## Download a UCF shared list

In order for compliance managers to download UCF authority documents from the UCF CCH, the list must be marked as Shared. When updating Authority Documents or adding new ones, you must update all your authority documents to ensure that the common controls framework remains in sync with the authority documents you are using.

Role required: sn\_compliance\_admin or sn\_compliance\_manager

---

**Note:** The current design of UCF supports the downloading of mandated and implied controls. The downloading of implementation controls is not supported. See the Unified Compliance Documentation [How do I distribute an authority document list to other accounts?](#)

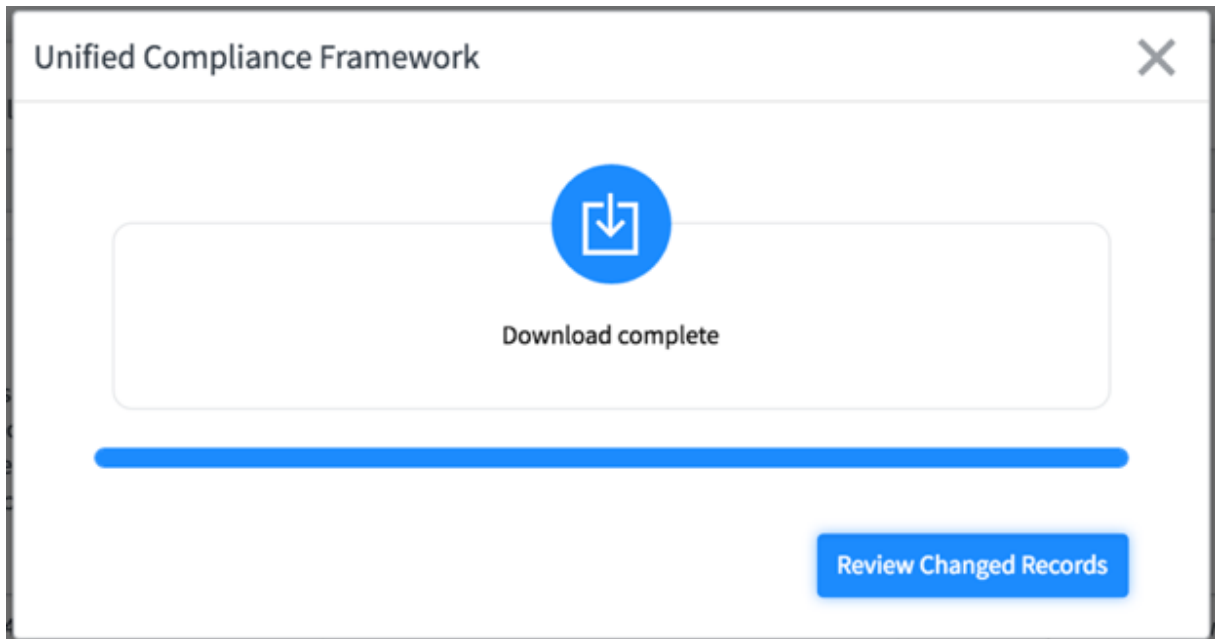
---



**Warning:** All data imported from UCF Authority Documents is read-only and must be protected. Do not customize the authority documents, citations, or policy statements on any UCF fields on the GRC tables.

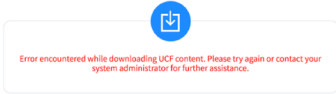
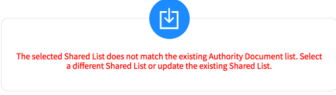
1. Navigate to Policy and Compliance Administration Unified Compliance Integration .
2. Click the UCF configuration.
3. [Configure the UCF integration](#) on page 43, if necessary.
4. Click Import Shared List.

A progress bar shows the progress of downloading and importing the documents.

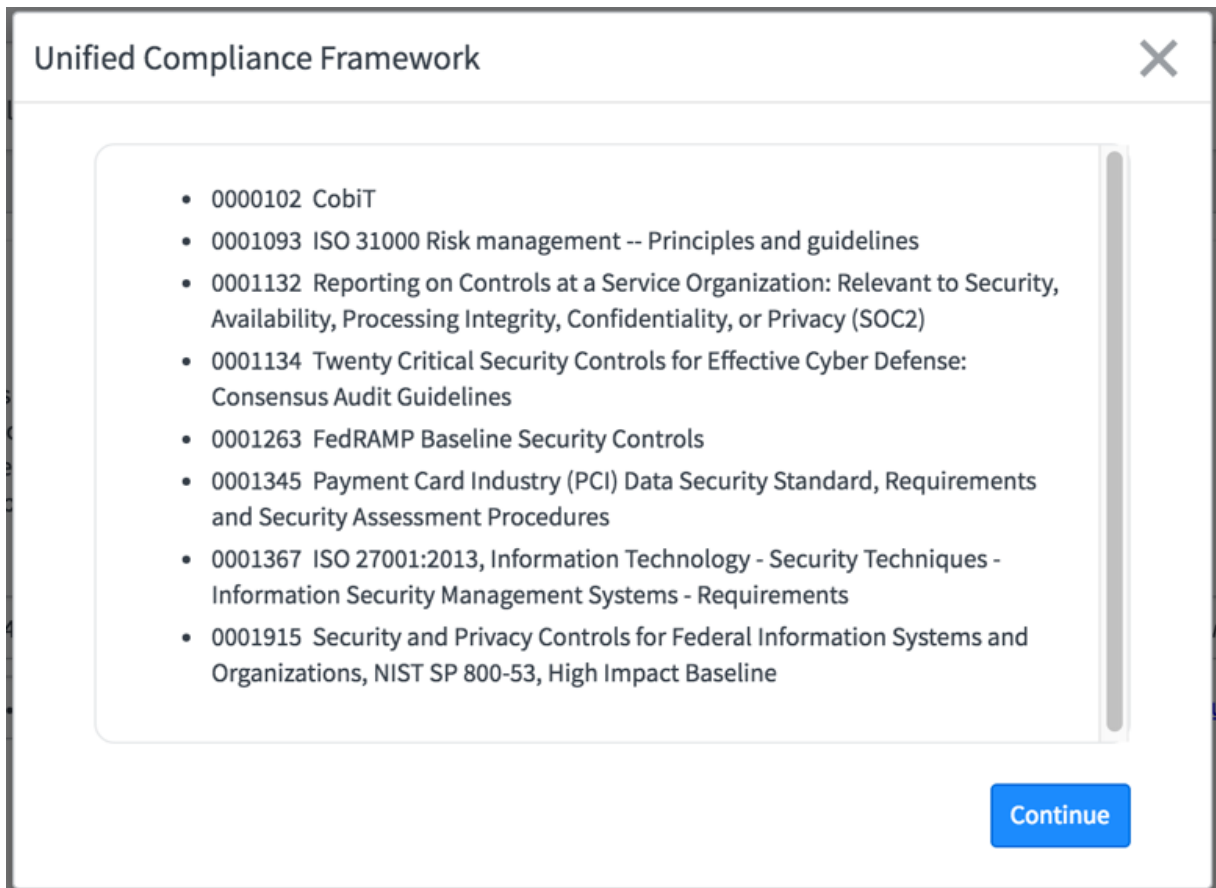


You may encounter any of the following errors:

**Table 18: UCF Shared List Errors**

Error	Explanation	Resolve
	<p>If the internet connection is lost for any reason, this message appears.</p>	<ol style="list-style-type: none"> <li>1. Click Import Shared List to download again.</li> </ol>
	<p>If the selected UCF Shared List that you are downloading does not include all the authority documents you have already downloaded, this message appears.</p>	<ol style="list-style-type: none"> <li>1. Return to the CCH and verify that the Shared List you are trying to download includes all the Authority Documents from the original import to your instance.</li> <li>2. Click Import Shared List to download again.</li> </ol>

5. Click Review Changed Records to review the list of changed records.



Authority documents in the UCF content are organized and mapped to their proper citations, which in turn are mapped to a common set of controls. The terminology between UCF and the GRC applications differ slightly as explained in the following table.



Table 19: Terminology differences

UCF	ServiceNow GRC application
Authority Document	Authority Document
Citation	Citation
Control	Policy Statement

## Controls

Controls are specific implementations of a policy statement. Retired controls do not appear in the list.

Controls inherit the Type, Category, and Classification from the policy statement. Controls are generated from the profile types that are assigned to a policy statement.

- My Controls are contained in the Controls module and contain active controls for which you are the owner. Retired controls do not appear in the list.
- All Controls are contained in the Controls module and contains all active controls. Retired controls do not appear in the list.

## Create a control

Controls are automatically generated when you associate a policy with a profile type or a profile type with a policy statement. A control is created for each profile listed in the profile type for the policy statement. Controls can also be manually created.

Role required: sn\_compliance.admin or sn\_compliance.manager

1. Navigate to Policy and Compliance Controls All Controls .
2. Click New.
3. Fill in the fields on the form, as appropriate.

Table 20: Control

Field	Description
Name	The name of the control.
Number	Read-only field that is automatically populated with a unique identification number.
Profile	The related profile.
Policy Statement	The related policy statement.
Owning group	Group that owns the policy.
Owner	User that owns the policy.  <b>Note:</b> The owner is always added as a respondent.

Field	Description
Key control	Marks the control as a key control.
Weighting	Set the weighting between 1 and 10. Used to calculate the control failure factor of a risk.
Status	<p>The control status is a read-only field. Possible choices are:</p> <ul style="list-style-type: none"> <li>• Compliant</li> <li>• Non compliant</li> <li>• Not applicable</li> </ul>
State	<p>The control state is a read-only field. Possible choices are:</p> <ul style="list-style-type: none"> <li>• Draft In this state, all compliance users can modify the control. Only available when creating a one-off control. One-off controls are possible but not recommended.</li> <li>• Attest When the control is created from a policy statement, controls are in this state.</li> </ul> <hr/> <p><b>Note:</b> When a control is set back to draft, the attestation is canceled.</p> <hr/> <ul style="list-style-type: none"> <li>• Review Controls are automatically moved to review from the attestation phase.</li> <li>• Monitor In this state, all compliance managers can move the control from review to monitor.</li> <li>• Retired Compliance managers or administrators can move a control from Monitor to Retired. Indicators do not run when the control is in this state.</li> </ul> <hr/> <p><b>Note:</b> When a control is retired, any attestation associated with it is canceled.</p> <hr/>
Enforcement	<p>Select from a list of options:</p> <ul style="list-style-type: none"> <li>• Mandated</li> <li>• Voluntary</li> </ul>

Field	Description
Category	<p>Select from a list of options:</p> <ul style="list-style-type: none"><li>• Acquisition or sale of facilities, technology, and services</li><li>• Audits and risk management</li><li>• Compliance and Governance Manual of Style</li><li>• Human Resources management</li><li>• Leadership and high level objectives</li><li>• Monitoring and measurement</li><li>• Operational management</li><li>• Physical and environmental protection</li><li>• Privacy protection for information and data</li><li>• Records management</li><li>• System hardening through configuration management</li><li>• Systems continuity</li><li>• Systems design, build, and implementation</li><li>• Technical security</li><li>• Third Party and supply chain oversight</li><li>• Root</li><li>• Deprecated</li></ul>

Field	Description
Type	Select from a list of options: <ul style="list-style-type: none"> <li>• Acquisition/Sale of Assets or Services</li> <li>• Actionable Reports or Measurements</li> <li>• Audits and Risk Management</li> <li>• Behavior</li> <li>• Business Processes</li> <li>• Communicate</li> <li>• Configuration</li> <li>• Data and Information Management</li> <li>• Duplicate</li> <li>• Establish Roles</li> <li>• Establish/Maintain Documentation</li> <li>• Human Resources Management</li> <li>• Investigate</li> <li>• IT Impact Zone</li> <li>• Log Management</li> <li>• Maintenance</li> <li>• Monitor and Evaluate Occurrences</li> <li>• Physical and Environmental Protection</li> <li>• Process or Activity</li> <li>• Records Management</li> <li>• Systems Continuity</li> <li>• Systems Design, Build, and Implementation</li> <li>• Technical Security</li> <li>• Testing</li> <li>• Training</li> </ul>
Classification	Select from a list of options: <ul style="list-style-type: none"> <li>• Preventive</li> <li>• Corrective</li> <li>• Detective</li> <li>• IT Impact Zone</li> </ul>
Frequency	Select from a list of options: <ul style="list-style-type: none"> <li>• Event Driven</li> <li>• Daily</li> <li>• Weekly</li> <li>• Monthly</li> <li>• Quarterly</li> <li>• Semi-Annually</li> <li>• Annually</li> </ul>
Description	A description of the control.
Additional Information	Additional information about the control.

Field	Description
Attestation	
Attestation	<p>Select from a list of options.</p> <ul style="list-style-type: none"> <li>• Other attestation types can be configured.</li> <li>• If this field is populated, then the Attestation Respondents field automatically becomes mandatory, and the owner is made the respondent.</li> </ul> <hr/> <p><b>Note:</b> If the user changes the attestation type in the policy statement, all the related controls are changed also.</p> <hr/>
Attestation respondents	<ul style="list-style-type: none"> <li>• Users assigned to the attestation of this control.</li> <li>• Only a user with the sn_grc.user role can be added as a respondent.</li> </ul> <hr/> <p><b>Note:</b> When both the Attestation and Attestation respondents fields are set, attestations are created when you click Attest.</p> <hr/>
Activity Journal	
Additional comments	

4. Click Submit.

## Follow a control

Connect integrates with Policy and Compliance Management providing an overlay to the standard interface, allowing users to participate in conversations while they work and collaborate on the control record.

Role required: sn\_compliance.user or sn\_compliance.reader

For more information about Connect, see [Connect](#).

1. Navigate to Policy and Compliance Controls All Controls .
2. Open the control record.
3. Click the Follow tab and select one of the options.

Option	Action
To add the Connect sidebar	<ul style="list-style-type: none"> <li>• Click Open Connect mini.</li> </ul>
To add the Connect full-screen view	<ul style="list-style-type: none"> <li>• Click Open Connect Full.</li> </ul>

## Attestations

Attestations are surveys that gather evidence to prove that a control is implemented. If the control's attestation field and respondents fields are set, then when a controls moves from the Draft state to the Attest state, a notification is sent to the attestation respondents.

Users can create multiple attestation types and set their policy statements to different attestations. A sample attestation called GRC Attestation is also provided as the default attestation which is composed of the following simple questions:

By default, GRC Attestation is used for controls and provides the following assessment questions:

- Is this control implemented?
- Attach evidence
- Explain

My Attestations module is in the Controls section of the . It contains all the active attestations which you are one of the respondents.

My Attestations is in the Controls section of the Policy and Compliance application and contains active attestations for which you are the respondent. The attestations appear in a list with a single attestation record per control.

All Attestations is contained in the Controls section of the Policy and Compliance application and contains all active attestations.

Compliance managers can create new attestation types containing different types of questions to fit their needs.

Compliance managers can create a new set of questions for each policy statement. See [Create an attestation type](#) on page 55.

### Attest a control

Controls start in a Draft state and when the user clicks Attest on a control form, the control moves to the Attest state and all the respondents receive an attestation.

Role required: sn\_grc.user

Attestations do not appear in the Self-Service My assessments & surveys module, because hundreds of GRC assessment records could be generated at once and should be separated from other assessments, in a separate list view.

1. Navigate to Policy and Compliance Controls My Attestations .
2. Open the attestation and review the details.

Option	Description
<b>If you are unable to answer the questions</b>	<ol style="list-style-type: none"> <li>1. Reassign the attestation to another user in the Assigned to field.</li> <li>2. Click Update and close the record.</li> </ol>

**Note:** Only a user with the sn\_grc.user role can be re-assigned the attestation.

The list of attestations refreshes when you reassign an attestation to another user.

Option	Description
<b>If you are able to answer the questions</b>	<ol style="list-style-type: none"> <li>1. Click Take attestation.</li> <li>2. Answer the questions and attach information, as required.</li> <li>3. Click Submit.</li> </ol> <p>The list of attestations refreshes when you close the Take Assessment pop-up window.</p>

## Create an attestation type

Rather than using the default GRC attestation type, the compliance manager can create a new set of questions for each policy statement.

Role required: sn\_compliance.attest\_creator or sn\_compliance.manager or sn\_compliance-admin

1. Navigate to Policy and Compliance Administration Attestation Types .
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 21: Assessment Metric Type**

Field	Description
Name	The name of the assessment type.
Assessment duration	
Table	
Scale factor	
Condition	
Description	
State	
Enforce condition	
Roles	

4. Click Submit.

## Attestation designer

The attestation designer provides a single interface that users can use to create, and edit attestations, as well as change scoring parameters.

All attestation records are stored in assessment tables and displayed in Attestation views of those tables.

The designer contains the following elements:

**Table 22: Elements of the Attestation Designer**

Element	Description
Controls	Controls for the supported question data types are available in the Controls palette. Drag a control onto the designer canvas to create a question of that type.
Header bar	The header bar contains tabs that display different views and a menu of various functions. The availability of each option depends on the status of the attestation that is opened in the designer.
Design canvas	New attestations open in the Design view. The attestation Name field appears above the first category in the canvas. A blank question field appears in the category container.

#### *Create a control attestation using the Attestation Designer*

Unlike other types of assessments, control attestations do not appear in the Self-Service My assessments & surveys module, because hundreds of control attestations could be generated at once. Instead, controls attestations are shown as a list in the My Attestations module and All Attestations module. The Attestation Designer includes a design canvas, a header bar, and many controls for creating attestations.

Role required: sn\_compliance.attest\_creator, sn\_compliance.manager, sn\_compliance.administrator

1. Navigate to Policy and Compliance Administration Attestation Types .
2. Click Attestation Designer.
3. Enter a name in the Name field above first category in the canvas.  
A blank question field appears in the category container.
4. Drag a control onto the designer canvas to create a question of that type.

**Table 23: Question controls**

Data type	Description	Scored
Attachment	Question with a Manage Attachments icon that allows users to attach one or more files.	Y
Boolean	Question with a check box or a Yes/No list for user responses.	
Choice	List of predefined options. For more information, see the definition for Choices.	Y
Date	Date field.	N
Date/Time	Date and time field.	N
Number	Number field with predefined minimum and maximum values. The default is 1-10.	N



Data type	Description	Scored
Percentage	Percentage field with a prescribed range.	N
Scale	Predefined <i>Likert scale</i> . Answer options appear as radio buttons.	Y
Numeric Scale	Selectable number scale. The default is 1-5. Answer options appear as radio buttons.	Y
String	Single or multiline text field.	N
Template	Choice list of templates that provide a predefined scale of options. .	Y
Reference	Choice list of fields from a specified reference table. This data type does not support reference qualifiers.	

**Note:** Set the correct answer for the metric that you want to be scored. Scored metrics determine the compliance status of the controls.

5. Click one of the following tabs to change the view in the canvas:

Option	Description
<b>Design</b>	Add categories and questions, and configure the properties of each. This is the default view of the canvas when you open the designer.
<b>Configuration</b>	Create introductions and end notes for attestations, and select a signature.
<b>Availability</b>	Select the recipients for each category in the attestation.

6. Point to the menu icon in the upper right of the Attestation Designer to select one of the following options:

**Note:** The availability of each option depends on the status of the attestation that is opened in the designer.

Option	Description
<b>Save</b>	Save the current attestation.
<b>Preview</b>	Display a preview to the selected recipients.
<b>Publish</b>	Distributes the attestation to the selected recipients.
<b>Save and Publish</b>	Saves and distributes the attestation in one step.
<b>New Attestation</b>	Opens a fresh canvas for a new attestation.

Option	Description
<b>Load Attestation</b>	Opens a list of existing attestations that you can select and edit.

## GRC issues management

Issues can be created manually to document audit observations, remediations, or to accept any problems. They are automatically generated from indicator results, attestation results, or control test effectiveness.

An issue is created automatically when:

- Issue - An indicator fails
- Control issue - A control attestation is completed indicating that the control is Not implemented
- Control test issue - A control test is closed complete with the control effectiveness set to Ineffective
- Other issue - is created by the user manually

Remediating an issue marks an intention to fix the underlying issue causing the control failure or risk exposure. Accepting an issue marks an intention to create an exception for a known control failure or risk. Controls that are Accepted remain in a non-compliant state until the control is reassessed. In this way, the issue can be used to document observations during audits.

## Create a GRC issue manually

Manually create issues to document audit observations, the intention of remediations, or to accept any problems.

Role required: (per product)

- In GRC: compliance\_admin, compliance\_manager, or sn\_compliance.user
- In Risk Management: \_admin, risk\_manager, or sn\_risk.user
- In Audit Management: audit\_admin, audit\_manager, or audit\_admin or sn\_audit.user

1. Navigate to one of the following locations:
  - Audit Issues Create New .
  - Policy and Compliance Issues Create New .
  - Risk Issues Create New .
2. Fill in the fields on the form, as appropriate.

**Table 24: Issue**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
State	<ul style="list-style-type: none"> <li>• New</li> <li>• Analyze</li> <li>• Respond</li> <li>• Review</li> <li>• Closed</li> </ul>

Field	Description
Assignment group	A group assigned to the issue.
Assigned to	The user assigned to the issue.
Priority	Priority for this issue: <ul style="list-style-type: none"> <li>• 1 - Critical</li> <li>• 2 - High</li> <li>• 3 - Moderate</li> <li>• 4 - Low</li> <li>• 5 - Planning</li> </ul>
Short description	Brief description of the issue.
Details	
Profile	The related profile.
Item	The related control or risk.
Description	A more detailed explanation of the issue.
Recommendation	The recommended action to resolve this issue.
Dates	
Planned start date	Date and time that work on the issue is expected to begin.
Planned end date	Date and time that work on the issue is expected to end.
Planned duration	Estimated amount of work time. Calculated using the Planned start date and Planned end date.
Actual start date	Time when work began on this issue
Actual end date	Time when work on this issue was completed.
Actual duration	Amount of work time. Calculated using the Actual start date and Actual end date.
Activity	
Work notes	Information about how to resolve the issue, or steps already taken to resolve it, if applicable. Work notes are visible to users who are assigned to the issue.
Additional comments (Customer visible)	Public information about the enhancement request.
Engagement	
Engagement	The related engagement.

3. Click Submit.

## GRC continuous monitoring

Continuous monitoring involves activities related to identifying and creating key risk and controls indicators. Supporting information can be collected for those indicators through automatic data collection or manual tasks. Indicator results are then used to create issues for controls, update risk scores, and provide supporting information for audit activities and control testing.

### Indicators

Indicators collect data to monitor controls and risks, and collect audit evidence. Indicators monitor a single control or risk.

### Indicator templates

Indicator templates allow the creation of multiple indicators for similar controls or risks.

## Create a GRC indicator

Indicator data for controls, risk, and audit evidence are measured differently depending on the GRC-related application.

Role required: compliance\_admin or compliance\_manager, risk\_admin or risk\_manager, audit\_admin or audit\_manager

1. Navigate to one of the following locations:
  - Policy and Compliance Indicators Indicators .
  - Risk Indicators Indicators .
  - Audit Indicators Indicators .
2. Select New.
3. Fill in the fields on the form, as appropriate.

**Table 25: Indicator**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
Active	Check box that determines whether the indicator is active.
Name	Name of the indicator.
Item	The related control or risk.
Template	The related indicator template.
Applies to	The profile related to the Item.
Owner	The indicator owner.
Owning group	The group that owns the indicator.

Field	Description
Override Template	Click to override the indicator template associated to this indicator
Last result passed	Read-only field indicating whether last result passed.
Schedule	
Collection frequency	Select the collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule.
Next run time	Read-only field that is automatically populated with the next collection time for indicator results.
Method	
Type	Results can be gathered manually using task assignment or automatically using basic filter conditions, Performance Analytics, or a script. <ul style="list-style-type: none"> <li>• Manual</li> <li>• Basic</li> <li>• Script</li> </ul>
Short Description	If Type is Manual, this field is present. Brief description of the issue.
Instructions	If Type is Manual, this field is present. Instructions for the collection of indicator results.
Value Mandatory	If Type is Manual, this field is present.
Passed/Failed	If Type is Basic, this field is present. Indicator passes or fails.
PA Threshold	If Type is PA Indicator, this field is present. The associated PA Threshold.
Script	If Type is Script, this field is present. Script that obtains the desired system information.
Supporting Data	
Table	Use supporting data to gather supporting evidence from other applications.
Supporting data fields	Supporting data fields based on the selected table.

## 4. Click Submit.

## Create a GRC indicator template

Compliance or risk managers create indicator templates from which many indicators can be created.

Role required: compliance\_admin or compliance\_manager, risk\_admin or risk\_manager, audit\_admin or audit\_manager

1. Navigate to one of the following locations:
  - Policy and Compliance Indicators Indicator Templates .
  - Risk Indicators Indicator Templates .
  - Audit Indicators Indicator Templates .
2. Select New.
3. Fill in the fields on the form, as appropriate.

**Table 26: Indicator template**

Field	Description
Name	Name of the indicator.
Active	Check box that determines whether the indicator template is active.
Content	The related policy or risk statement.
Schedule	
Collection frequency	Select the collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule.
Next run time	Read-only field that is automatically populated with the next collection time for indicator results.
Method	
Type	Results can be gathered manually using task assignment or automatically using basic filter conditions, Performance Analytics, or a script. <ul style="list-style-type: none"> <li>• Manual</li> <li>• Basic</li> <li>• PA Indicator</li> <li>• Script</li> </ul>
Short Description	If Type is Manual, this field is present. Brief description of the issue.
Instructions	If Type is Manual, this field is present. Instructions for the collection of indicator results.
Value Mandatory	If Type is Manual, this field is present.

Field	Description
Passed/Failed	If Type is Basic, this field is present. Indicator passes or fails.
PA Threshold	If Type is PA Indicator, this field is present. The associated PA Threshold.
Script	If Type is Script, this field is present. Script that obtains the desired system information.
Supporting Data	
Collect Supporting Data	Check to gather supporting evidence from other applications.

4. Click Submit.

## GRC PA Indicators

GRC PA Indicators link GRC content and items to Performance Analytics indicators, breakdowns and thresholds. You can associate Performance Analytics indicators with risk statements, risks, policy statements, and controls to view scorecards and trends and analyze current conditions and trends.

The risks and controls associated with a PA indicator or PA indicator/breakdown/element automatically monitor any PA threshold with the same PA indicator or PA indicator, breakdown, or element relationship. Any PA threshold breach is reported at the risk or control and Performance Analytics indicators relationship level within a breach counter. See [Performance Analytics](#).

### PA threshold breach impact

When a risk or control and Performance Analytics indicators relationship breach counter is different than zero (for example, a PA threshold with the same PA indicator or PA indicator, breakdown, or element relationship has breached), and if no opened issue already exists, then an issue is created which is associated to the risk or control. Additionally for risks, the Indicator failure factor represents the number of risk and Performance Analytics indicators relationships with a breach counter different than zero.

### Reset all PA Indicator breach counters

Reset breach counters associated to a risk or control by clicking Reset all PA Indicator breach counters or opening the specific relationship and clicking Reset Breach Counter.

### GRC PA indicator breach reports

There are two reports for the reporting of breaches:

- Risk PA Indicator Breaches
- Control PA Indicator Breaches

## Upgrade from Helsinki to Istanbul

After upgrading an instance from Helsinki to Istanbul, activate the GRC: Performance Analytics Premium Integration plugin. After doing so, every GRC indicator of type pa\_Indicator is migrated to the new GRC PA Integration and de-activated. The GRC indicators of type pa\_indicator is deactivated to avoid duplicate PA threshold events. If you prefer to continue using the GRC Indicator of type pa\_indicator, activate them again and deactivate the GRC PA Integration records that were created during the migration.

The trend in the PA indicator relationship shows only when the PA indicator has the Publish on Scorecards flag on. Otherwise no score is always displayed.

## Activate GRC: Performance Analytics Premium Integration

The GRC: Performance Analytics Premium Integration plugin provides an integration between Performance Analytics and the Risk Management and Policy and Compliance Management applications, providing more insight into organizational risk and compliance performance.

Role required: admin

This plugin includes demo data and activates related plugins if they are not already active.

1. Navigate to System Definition Plugins .
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

If the plugin has optional features that are not functional because other plugins are inactive, those plugins are listed. A warning states that some files are not installed. If you want the optional features to be installed, cancel this activation, activate the necessary plugins, and then return to activating the plugin.

4. If available, select the Load demo data check box.

Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.

5. Click Activate.

After activating the GRC: Performance Analytics Premium Integration plugin on an instance with customized related lists on content (risk or policy statement) or items (risk or control), you may have to manually add the PA Indicator to content relationships and/or the PA indicator to item relationships.

## Associate a Performance Analytics indicator with GRC content

You can associate Performance Analytics indicators with risk statements and policy statements to analyze trends related to the risk or policy.

Role required: sn\_risk.manager or sn\_compliance.manager

1. Navigate to one of the following locations:
  - Policy and Compliance Policies and Procedures Policy Statements .
  - Risk Risk Library Risk Statements .
2. Open a risk statement or policy statement.



3. In the PA Indicators related list, click New.
4. Fill in the fields on the form, as appropriate.

Table 27: PA Indicators

Field	Description
PA Indicator*	The performance analytics indicator to associate the Risk Statement or Policy Statement with.

5. Click Submit.  
On the risk statement or policy statement form, in the PA Indicators related list, you see the associated indicator. You can optionally click View Indicator on the desired indicator to see the indicator's Performance Analytics scorecard. The PA Indicator associations are carried over to all risks or controls associated to the original risk statement or policy statement. Additionally, if the indicator has a breakdown that matches the risk or control's profile (for example a Business Service breakdown), the Breakdown and Element fields for the relationship are automatically filled in.

## Associate a Performance Analytics indicator with a GRC item

You can associate Performance Analytics indicators with risks and controls to analyze trends related to the profile that risk or control belongs to.

Role required: sn\_risk.manager or sn\_compliance.manager

1. Navigate to one of the following locations:
  - Policy and Compliance Controls All Controls .
  - Risk Risk Register All Risks .
2. Open a risk or control.
3. In the PA Indicators related list, click New.
4. Fill in the fields on the form, as appropriate.

Table 28: PA Indicators

Field	Description
PA Indicator*	The performance analytics indicator to associate the Risk or Control with.
Breakdown	Select a breakdown to view a specific trend based on the breakdown element.
Element	Select the breakdown element to view a particular trend and scorecard.  <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p><b>Note:</b> This field is dependent on the Breakdown field is populated. When visible, it is mandatory.</p> </div> <p>Note: This field is only visible if the Breakdown field is populated. It is mandatory when visible</p>

**5. Click Submit.**

On the Risk or Control form, in the PA Indicators related list, you see the associated indicator. You can optionally click View Indicator on the desired indicator to see the indicator's Performance Analytics scorecard.

## Update associated GRC indicators for a set of items

You can update all of the items belonging to a GRC content record so each item is individually related to the PA indicator.

Role required: sn\_risk.manager or sn\_compliance.manager

**1. Navigate to one of the following locations:**

- Policy and Compliance Policies and Procedures Policy Statements .
- Risk Risk Library Risk Statements .

**2. Open a Risk Statement or Policy Statement that has an associated Performance Analytics Indicator.****3. Click the Update PA Relationships related link.**

All of the risks or controls related to the risk statement or policy statement are automatically associated with all of the risk statement or policy statement's indicators. Additionally, if the indicator has a breakdown that matches the risk or control's profile (for example a Business Service breakdown), the Breakdown and Element fields for the relationship are automatically filled in.

## Policy and Compliance Administration

The Policy and Compliance Management application provides properties associated with article templates, attestation types, and UCF integration.

### Article Templates

Policy and Compliance managers can create templates for policy article publishing.

### Attestation Types

Rather than using the default GRC attestation type, the compliance manager can create a new set of questions for each policy statement.

### Unified Compliance Integration

See [Configure the UCF integration](#) on page 43.

## Create a GRC article template

Policy and Compliance managers can create templates for policy article publishing.

Role required: sn\_audit.manager

- 1. Navigate to Policy and Compliance Administration Article Templates .**
- 2. Click New.**
- 3. Fill in the fields on the form, as appropriate.**

Table 29: Authority Document

Field	Value
Name	Name of the article template.
Type	<ul style="list-style-type: none"> <li>• Script</li> <li>• HTML</li> <li>• XML</li> </ul>
Script	The script code. This field is dependent on the Type field.
HTML	The HTML code. This field is dependent on the Type field.
XML	The XML code. This field is dependent on the Type field.
Is default	Check box to indicate that this template is used as the default template for all KB articles.

4. Click Submit.

## Risk Management

The ServiceNow® Risk Management application provides a centralized process to identify, assess, respond to, and continuously monitor Enterprise and IT risks that may negatively impact business operations. The application also provides structured workflows for the management of risk assessments, risk indicators, and risk issues.

The GRC: Risk Management (com.sn\_compliance) plugin is available as a separate subscription and requires activation.

### Explore

- [GRC Common Release notes](#)
- [Risk Management Release notes](#)
- [Upgrade to Istanbul](#)

### Set up

- [Activate Risk Management](#) on page 68
- [Configure Risk Management](#) on page 68

### Administer

- [Risk Management Administration](#) on page 114

### Use

- [GRC Workbench](#) on page 79
- [Risk Register](#) on page 95

### Develop

- [Developer training](#)
- [Developer documentation](#)
- [Components installed with Risk Management](#) on page 68

### Integrate

- [GRC PA Indicators](#) on page 63

### Troubleshoot and get help

- [Ask or answer questions in the GRC community](#)

- [Search the HI Knowledge Base for known error articles](#)
- [Contact ServiceNow Support](#)

## Activate Risk Management

The GRC: Risk Management (com.sn\_risk) plugin is available as a separate subscription.

Role required: admin

This plugin includes demo data and activates related plugins if they are not already active.

1. Navigate to [System Definition Plugins](#) .
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the [Activate/Upgrade](#) related link.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

If the plugin has optional features that are not functional because other plugins are inactive, those plugins are listed. A warning states that some files are not installed. If you want the optional features to be installed, cancel this activation, activate the necessary plugins, and then return to activating the plugin.

4. If available, select the [Load demo data](#) check box.

Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the [Load Demo Data Only](#) related link on the System Plugin form.

5. Click [Activate](#).

## Configure Risk Management

Administrators in the global domain can set properties to determine how the system defines the Risk Management application.

Role required: sn\_risk.admin

---

**Note:** Administrators in domains lower than the global domain can view the Properties screen, but cannot modify the settings.

---

1. Navigate to [Risk Administration Properties](#) .
2. Fill in the fields on the Risk Management Properties form. See [Properties installed with Risk Management](#) on page 69 for property descriptions.
3. Click [Save](#).

## Components installed with Risk Management

Activating the GRC: Risk Management (com.sn\_risk) plugin adds or modifies several tables, user roles, and other components.

## Tables installed with Risk Management

GRC: Risk Management adds the following tables.

Table	Description
Risk [sn_risk_risk]	Extends Item [sn_grc_item] and stores specific risks associated with profiles
Risk Criteria [sn_risk_criteria]	Stores risk criteria used to calculate risk scores
Risk Statement [sn_risk_definition]	Extends Content [sn_grc_content] and stores definitions of risks.
Risk Framework [sn_risk_framework]	Extends Document [sn_grc_document] and stores all risk frameworks, a collection of risk statements
Risk Framework to Profile Type [sn_risk_m2m_framework_profile_type]	Extends Document to Profile Type [sn_grc_m2m_document_profile_type] and is a many-to-many relationship table that is used to manage the relationships between risk frameworks and profile types
Risk to Control [sn_risk_m2m_risk_control]	Stores many-to-many relationships between risks and controls
Profile Type to Risk Statement [sn_risk_m2m_risk_definition_profile_type]	Extends Content to Profile Type [] and is a many-to-many relationship table that is used to manage the relationships between profile types and risk statements
Risk Relationship sn_risk_m2m_risk_risk	Stores many-to-many relationships between risks
Risk Tasks [sn_risk_m2m_risk_task]	Stores many-to-many relationships between risks and tasks

---

**Note:** All additional tables installed by the dependent plugins are also needed for GRC: Risk Management.

---

## Properties installed with Risk Management

GRC: Risk Management adds the following properties.

Name	Description
States for which the risk is active (the first state is the default active state) sn_risk.active_states	<ul style="list-style-type: none"> <li>Type: string</li> <li>Default value: draft, assess, review, monitor</li> <li>Location: Risk Administration Properties</li> </ul>

Name	Description
States for which risk is inactive (the first state is the default inactive state) sn_risk.closed_states	<ul style="list-style-type: none"> <li>Type: string</li> <li>Default value: retired</li> <li>Location: Risk Administration Properties</li> </ul>
Name of the assessment metric type that is used for risk assessment sn_risk.default_assessment	<ul style="list-style-type: none"> <li>Type: string</li> <li>Default value: Risk Assessment</li> <li>Location: Risk Administration Properties</li> </ul>
sn_risk.glide.script.block.client.globals	<ul style="list-style-type: none"> <li>Type: true or false</li> <li>Default value: False</li> <li>Location: Risk Administration Properties</li> </ul>
Use qualitative impact scores as input sn_risk.qualitative_impact	<ul style="list-style-type: none"> <li>Type: true   false</li> <li>Default value: false</li> </ul> <hr/> <p><b>Note:</b> After an upgrade, this value is set to true.</p> <hr/> <ul style="list-style-type: none"> <li>Location: Risk Administration Properties</li> </ul>
Use qualitative likelihood scores as input sn_risk.qualitative_likelihood	<ul style="list-style-type: none"> <li>Type: true   false</li> <li>Default value: false</li> <li>Location: Risk Administration Properties</li> </ul>
A list of tables (comma separated) that are available in the 'Applies to' field on the Risk form. Add .extended after the table name to include all extended tables. sn_risk.risk_applies_to_tables	<ul style="list-style-type: none"> <li>Type: string</li> <li>Default value: core_company, cmn_location.extended, task.extended, cmdb_ci_service, cmdb_ci_appl.extended, cmdb_ci_database.extended, cmdb_ci_hardware.extended, grc_condition_collection, cert_filter</li> <li>Location: Risk Administration Properties</li> </ul>

## Roles installed with Risk Management

GRC: Risk Management adds the following roles.

Role title [name]	Description	Contains roles
Risk User [sn_risk.user]	Contains the reader and user roles in sn_grc scopes, and the reader role in the Risk Management application. In addition to the inherited permissions, the risk user can view profile types, profiles, risks, and remediation tasks. The risk user can be assigned risks and has read-only access to the Policy and Compliance Management application and modules.	<ul style="list-style-type: none"> <li>• sn_grc.reader</li> <li>• sn_grc.user</li> <li>• sn_risk.reader</li> <li>• Inherits the following roles if the GRC: Policy and Compliance Management plugin is activated.               <ul style="list-style-type: none"> <li>• grc_compliance_reader</li> <li>• grc_user</li> <li>• grc_audit_reader</li> <li>• grc_control_test_reader</li> <li>• task_editor</li> </ul> </li> </ul>
Risk Reader [sn_risk.reader]	Contains the reader role in sn_grc scopes. In addition to the inherited permissions, the risk reader has read-only access rights to the Risk application and modules and can be assigned risks.	<ul style="list-style-type: none"> <li>• sn_grc.reader</li> </ul>
Assessment Creator [sn_risk.asmt_creator]		<ul style="list-style-type: none"> <li>• sn_grc.reader</li> <li>• sn_grc.user</li> <li>• sn_grc.manager</li> <li>• sn_risk.reader</li> <li>• sn_risk.user</li> <li>• Inherits the following roles if the GRC: Policy and Compliance Management plugin is activated.               <ul style="list-style-type: none"> <li>• grc_audit_reader</li> <li>• task_editor</li> <li>• certification_admin</li> <li>• grc_test_definition_admin</li> <li>• grc_control_test_reader</li> <li>• assessment_admin</li> <li>• certification</li> <li>• grc_compliance_reader</li> <li>• certification_filter_admin</li> <li>• grc_user</li> </ul> </li> </ul>

Role title [name]	Description	Contains roles
Risk Manager [sn_risk.manager]	Contains the reader, user, and manager roles in sn_grc scopes, and the reader and user roles in theRisk Management application. In addition to the inherited permissions, the risk manager can create risk frameworks, risk statements, and risks.	<ul style="list-style-type: none"> <li>• sn_grc.reader</li> <li>• sn_grc.user</li> <li>• sn_grc.manager</li> <li>• sn_risk.reader</li> <li>• sn_risk.user</li> <li>• Inherits the following roles if the GRC: Policy and Compliance Management plugin is activated.               <ul style="list-style-type: none"> <li>• grc_audit_reader</li> <li>• task_editor</li> <li>• certification_admin</li> <li>• grc_test_definition_admin</li> <li>• grc_control_test_reader</li> <li>• assessment_admin</li> <li>• certification</li> <li>• grc_compliance_reader</li> <li>• certification_filter_admin</li> <li>• grc_user</li> </ul> </li> </ul>
Risk Admin [sn_risk.admin]	Contains the reader, user, manager, and admin roles in sn_grc scopes, and the reader, user, and manager roles in theRisk Management application. In addition to the inherited permissions, the risk admin can delete risk frameworks, risk statements, and risks, and modify admin properties and risk criteria.	<ul style="list-style-type: none"> <li>• sn_grc.reader</li> <li>• sn_grc.user</li> <li>• sn_grc.manager</li> <li>• sn_grc.admin</li> <li>• sn_risk.reader</li> <li>• sn_risk.user</li> <li>• sn_risk.manager</li> <li>• Inherits the following roles if the GRC: Policy and Compliance Management plugin is activated.               <ul style="list-style-type: none"> <li>• grc_audit_reader</li> <li>• task_editor</li> <li>• certification_admin</li> <li>• grc_test_definition_admin</li> <li>• grc_control_test_reader</li> <li>• assessment_admin</li> <li>• certification</li> <li>• grc_compliance_reader</li> <li>• certification_filter_admin</li> <li>• grc_admin</li> <li>• grc_user</li> </ul> </li> </ul>



## Client scripts installed with Risk Management

GRC: Risk Management adds the following client scripts.

Client script	Table	Description
Calculate Inherent ALE when ARO changes	Risk [sn_risk_risk]	Calculate the inherent Annualized Loss Expectancy (ALE) when the inherent Annual Rate of Occurrence (ARO) changes.
Calculate Inherent ALE when SLE changes	Risk [sn_risk_risk]	Calculate the inherent ALE when the inherent Single Loss Expectancy (SLE) changes.
Calculate Residual ALE when ARO changes	Risk [sn_risk_risk]	Calculate Residual ALE when Residual ARO changes.
Calculate Residual ALE when SLE changes	Risk [sn_risk_risk]	Calculate Residual ALE when Residual SLE changes.
Calculated ALE (Inherent ALE)	Risk [sn_risk_risk]	Updates the calculated ALE when the inherent ALE changes
Calculated ALE (Residual ALE)	Risk [sn_risk_risk]	Updates the calculated ALE when the residual ALE changes
Hide risk to control related list	Risk [sn_risk_risk]	Hides the Risk to Control Related List when compliance is not installed
Set maximum value (currency max value)	Risk Criteria [sn_risk_criteria]	Updates the maximum value when the currency max value field changes
Set maximum value (percentage max value)	Risk Criteria [sn_risk_criteria]	Updates the maximum value when the percentage max value field changes
Show risk generation message	Profile Type sn_grc_profile_type	Display business rule that shows a message indicating that risks are being generated when risks are being created for all the profiles in a profile type
Update Fields from Definition	<ul style="list-style-type: none"> <li>Risk [sn_risk_risk]</li> <li>Risk [grc_risk]</li> </ul>	Updates various fields from the risk statement whenever the risk statement field changes
Update Inherent Score (Inher Likelihood)	Risk [sn_risk_risk]	Updates the inherent score when the inherent likelihood changes
Update Inherent Score (Inherent impact)	Risk [sn_risk_risk]	Updates the inherent score when the inherent impact changes

Client script	Table	Description
Update Inherent Score (Likelihood)	Risk [grc_risk]	Updates the inherent score when the likelihood changes
Update Inherent Score (Significance)	Risk [grc_risk]	Updates the inherent score when the significance changes
Update Residual Score (Likelihood)	Risk [grc_risk]	Updates the residual score when the residual likelihood changes
Update Residual Score (Resid Likelihood)	Risk [sn_risk_risk]	Updates the residual score when the residual likelihood changes
Update Residual Score (Residual impact)	Risk [sn_risk_risk]	Updates the residual score when the residual impact changes
Update Residual Score (Significance)	Risk [grc_risk]	Updates the residual score when the residual significance changes
Use qualitative impact	<ul style="list-style-type: none"> <li>Risk [sn_risk_risk]</li> <li>Risk Statement [sn_risk_definition]</li> </ul>	Choose to show Inherent impact or inherent SLE based on the qualitative_impact system property.
Use qualitative likelihood	<ul style="list-style-type: none"> <li>Risk [sn_risk_risk]</li> <li>Risk Statement [sn_risk_definition]</li> </ul>	Choose to show Inherent impact or inherent SLE based on the qualitative_impact system property.
Validate Default Inherent SLE	Risk Statement [sn_risk_definition]	Validates that the inherent SLE is greater than or equal to the residual SLE when inherent SLE changes
Validate Default Residual ARO	Risk Statement [sn_risk_definition]	Validates that the inherent ARO is greater than or equal to the residual ARO when residual ARO changes
Validate Inherent ARO	Risk [sn_risk_risk]	Validates that the inherent ARO is greater than or equal to the residual ARO when inherent ARO changes
Validate Inherent impact	<ul style="list-style-type: none"> <li>Risk [sn_risk_risk]</li> <li>Risk Statement [sn_risk_definition]</li> </ul>	Validates that the inherent impact is greater than or equal to the residual impact when inherent impact changes

Client script	Table	Description
Validate Inherent likelihood	<ul style="list-style-type: none"> <li>Risk [sn_risk_risk]</li> <li>Risk Statement [sn_risk_definition]</li> <li>Risk [grc_risk]</li> </ul>	Validates that the inherent likelihood is greater than or equal to the residual likelihood when inherent likelihood changes
Validate Inherent Residual SLE	Risk Statement [sn_risk_definition]	Validates that the inherent SLE is greater than or equal to the residual SLE when residual SLE changes
Validate Inherent significance	Risk [grc_risk]	Validates that the inherent significance is greater than or equal to the residual significance when inherent significance changes
Validate Inherent SLE	Risk [sn_risk_risk]	Validates that the inherent SLE is greater than or equal to the residual SLE when inherent SLE changes
Validate Residual ARO	Risk [sn_risk_risk]	Validates that the inherent ARO is greater than or equal to the residual ARO when residual ARO changes
Validate Residual impact	<ul style="list-style-type: none"> <li>Risk [sn_risk_risk]</li> <li>Risk Statement [sn_risk_definition]</li> </ul>	Validates that the inherent impact is greater than or equal to the residual impact when residual impact changes
Validate residual likelihood	<ul style="list-style-type: none"> <li>Risk [sn_risk_risk]</li> <li>Risk Statement [sn_risk_definition]</li> <li>Risk [grc_risk]</li> </ul>	Validates that the inherent likelihood is greater than or equal to the residual likelihood when residual likelihood changes
Validate Residual significance	Risk [grc_risk]	Validates that the inherent significance is greater than or equal to the residual significance when residual significance changes
Validate Residual SLE	Risk [sn_risk_risk]	Validates that the inherent SLE is greater than or equal to the residual SLE when residual SLE changes

Script includes installed with Risk Management

GRC: Risk Management adds the following script includes.

Script include	Description
RiskALECalculator	Calculates Risk Annualized Loss Expectancy (ALE) based on Single Loss Expectancy (SLE) and Annual Rate of Occurrence (ARO) selections.
RiskGeneratorStrategy	Generates risks when relationships are created between profile types, risk definitions, and risk statements
RiskMigrationUtils	Utilities for migrating risks from grc_risk to sn_risk_risk.
RiskUtils	Editable script include that allows RiskUtilsBase to be overridden without affecting the base code.
RiskUtilsAJAX	Provides client-callable risk methods.
RiskUtilsAJAX2	Provides client-callable risk methods.
RiskUtilsBase	Provides base risk utilities. This protected script include cannot be edited.
RiskUtilsBaseV2	Risk utility base for Risk V2.
RiskUtilsV2	Risk utilities for Risk V2.

## Business rules installed with Risk Management

GRC: Risk Management adds the following business rules.

Business rule	Tables	Description
Assign risks to profiles	Profile [sn_grc_profile]	Allows the system to assign risks to various profiles.
Calculate qualitative scores	Risk [sn_risk_risk]	Calculates the inherent and residual scores for the risk and updates the qualitative values.
Calculate Scores	Risk [grc_risk]	Calculates the inherent, residual, and calculated risk score from the likelihood and significance of a risk.
Calculated ALE	Risk [sn_risk_risk]	Sets the calculated score for the risk.
Cascade Changes	Risk Statement [sn_risk_definition]	Copies changes to the name, description, and category fields from the risk statement to its associated risks.
Create risk scratchpad	Profile Type [sn_grc_profile_type]	Sets a scratchpad field to determine if risks are currently being created.

Business rule	Tables	Description
Populate SLE & ARO from definition	Risk [sn_risk_risk]	Populates the default values from the risk statement into a risk when a risk is created.
Prevent adding inactive framework	Risk Framework to Profile Type [sn_risk_m2m_framework_profile_type]	Prevents the association of an inactive risk framework with any profile type.
Prevent adding inactive risk statement	Risk Statement to Profile Type [sn_risk_m2m_definition_profile_type]	Prevents the association of an inactive risk statement with any profile type.
Rollup Profile Scores	<ul style="list-style-type: none"> <li>Profile [sn_grc_profile]</li> <li>Risk [grc_risk]</li> </ul>	Calculates inherent, residual, and calculated risk scores from the likelihood and significance of all risks associated with a profile.
Scratchpad: Risk Scoring	Risk [sn_risk_risk]	Sets scratchpad fields to determine if qualitative scoring is used for impact and likelihood and whether the compliance plugin is installed.
Scratchpad: Risk Statement Scoring	Risk Statement [sn_risk_definition]	Sets scratchpad fields to determine if qualitative scoring is used for impact and likelihood.
Set Content	Risk Statement to Profile Type [sn_risk_m2m_definition_profile_type]	Sets the content field to be equal to the risk statement in the many-to-many relationship.
Set maximum value	Risk Criteria [sn_risk_criteria]	Updates the maximum value whenever the currency or percentage max values change.
Sync between content and definition	Risk [sn_risk_risk]	Synchronizes the content and risk statement fields.
Sync qualitative fields	<ul style="list-style-type: none"> <li>Risk Statement [sn_risk_definition]</li> <li>Risk [sn_risk_risk]</li> </ul>	Synchronizes the qualitative and quantitative scores whenever risk impact, residual impact, inherent SLE, residual SLE, likelihood, residual likelihood, inherent ARO, or residual ARO change.
Update impact/likelihood	Risk Criteria [sn_risk_criteria]	Updates the SLE, ARO, impact, likelihood of all risk statements and risks that are using the risk criteria.
Update applies to when profile changes	Risk [grc_risk]	Updates the 'applies to' field on the risk form when the profile is changed on the risk form.

Business rule	Tables	Description
Update risk control factor	Risk to Control [sn_risk_m2m_risk_control]	Updates the risk control failure factor whenever a many-to-many relationship between risks and controls is created, updated, or deleted.
Validate inherent and residual values	Risk Statement [sn_risk_definition]	Validates that the inherent impact, likelihood, SLE, and ARO are greater than or equal to the corresponding residual values.
Validate residual fields	Risk [sn_risk_risk]	Validates that the inherent impact, likelihood, SLE, and ARO are greater than or equal to the corresponding residual values.

## Risk Management process

The Risk Management application provides a centralized process to identify, assess, respond to, and continuously monitor Enterprise and IT risks that may negatively impact business operations. The application also provides structured workflows for the management of risk assessments, risk indicators, and risk issues.

The Risk Management application follows a standard process:

1. Ensure that the settings for risk criteria and properties are correct based on the needs of your organization. Modify if necessary.
2. Create profile types to group common profiles with similar risks together for easier assessment.
3. Create risk statements to define a set of potential risks that could occur across the organization.
4. Assign risk statements to profile types, to generate risks from statements, or generate risks manually.
5. Determine the appropriate risk response (for example, Accept, Avoid, Mitigate, or Transfer), and document the justification for the response.
6. Assign and complete Remediation Tasks to ensure that risk mitigation efforts are implemented.
7. Utilize the Governance, Risk, and Compliance (GRC) application to track risk mitigation efforts by relating a risk to controls or policies which mitigate the risk.

## Risk Overview

The Risk Overview is contained in the Risk Management application and provides an executive view, allowing risk managers to quickly identify areas of concern by pinpointing profiles with known high risk.

The Policies and Procedures overview contains the following reports in the base system.

**Table 30: Risk Overview**

Name	Visual	Description
Inherent Risk		

Name	Visual	Description
Residual Risk		
Inherent Annual Loss Exposures		
Residual Annual Loss Exposures		
Risk Issues by Framework (Opened Date)		
Risks by Response		
Risk Expectations		
Profile	Drop down list	Select one or many profiles to view and compare their risks.
GRC - Risk States	Check boxes	Select one or many risk states to view and compare.
Risks by Category		
Very High Risk	Single Score	Displays the number of very high risks.
High Risk	Single Score	Displays the number of high risks.
Moderate Risk	Single Score	Displays the number of moderate risks.
Low Risk	Single Score	Displays the number of low risks.
Very Low Risk	Single Score	Displays the number of very low risks.
Inherent Risk Heatmap		
Residual Risk Heatmap		

## GRC Workbench

The GRC Workbench gives GRC administrators a graphical interface to create profile and risk dependencies. These relationships enable consistent risk mapping and modeling across the enterprise.

Access the GRC Workbench by navigating to [Risk GRC Workbench](#) .

---

**Note:** The GRC Workbench does not work with Legacy GRC.

---

### Model Setup Tab

The Model Setup tab contains links to perform the following tasks.

Link	Action
Dependency Model	Create profile classes and develop the organizational relationship model
Profile Types	Create and edit profile types
Dependency Map	Create and visualize profile relationships

## Risk Dependencies tab

The Risk Dependencies tab contains links to perform the following tasks.

Link	Action
Risk Frameworks	Create and edit risk frameworks
Risk Statements	Create and edit risk statements
Relationships	Create and visualize risk relationships

## Activate GRC Workbench

The GRC: Workbench plugin is not activated by default, it is available as a separate subscription within the GRC Suite.

Role required: admin

To create profile classes, profile dependencies, and risk dependencies using the GRC Workbench, activate the GRC: Risk Management plugin [com.sn\_risk] and the GRC: Profiles plugin [com.sn\_grc].

This plugin includes demo data and activates related plugins if they are not already active.

1. Navigate to System Definition Plugins .
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

If the plugin has optional features that are not functional because other plugins are inactive, those plugins are listed. A warning states that some files are not installed. If you want the optional features to be installed, cancel this activation, activate the necessary plugins, and then return to activating the plugin.

4. If available, select the Load demo data check box.

Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.

5. Click Activate.

## Create profile class using the GRC workbench

GRC managers create profile classes representing the types of things that will be part of the dependency model. Reports can be filtered to define relationships between the different profile classes. A profile class



defines what a profile actually is. It differs from a profile type (for example, Business Services and Critical Business Services), in that a profile can belong to many profile types but a profile can have only one profile class (for example, Business Service).

Role required: sn\_grc\_manager

1. Navigate to Risk GRC Workbench .
2. On the left, in the Profile classes section, click Add Class.
3. Enter a profile class name and click the plus (+) icon

The newly created profile class is added to the list on the left.

[Create relationships between profile classes using the GRC workbench](#) on page 81.

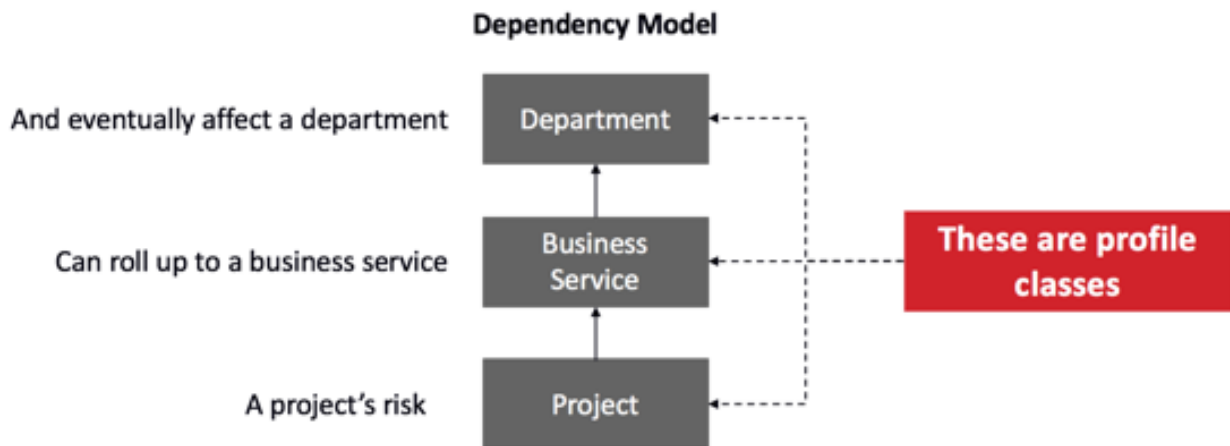
## Create relationships between profile classes using the GRC workbench

Managers create relationships between profile classes using the GRC workbench to build out the dependency map and better understand how profiles relate to one another.

Role required: sn\_grc.manager

[Create profile class using the GRC workbench](#) on page 80, before creating relationships between profile classes.

Profile classes can roll up to each other, leading to the development of the dependency model.



**Figure 4: Profile classes dependency model**

1. Navigate to Risk GRC Workbench .
2. Select the Model Setup tab at the top, and select the Dependency Model tab below.
3. If needed, create profile classes.
4. Do one of the following actions:

Option	Description
<b>If there are no relationships between profile classes</b>	Drag a profile class from the left to the center and drop it.

Option	Description
<b>If there are relationships between profile classes</b>	<p>Drag additional profile classes from the list on the left and drop them on the top or bottom of any profile class in the tree.</p> <hr/> <p><b>Note:</b> Dragging to the top of a profile class makes the target profile class roll up to the class that is dropped. Dragging to the bottom of a profile class makes the class that is being dropped roll up to the target class.</p>

---

**Note:** As long as you remain on the GRC workbench, click Undo after creating a relationship between profile classes to roll back the change. Leaving the GRC Workbench causes the undo history to be lost.

---

After modeling out profiles, define the risks in your organization:

- [Generate a risk from a risk framework](#) on page 96
- [Generate a risk from a risk statement](#) on page 96
- [Associate a risk framework or risk statement with a profile type to generate risks](#) on page 95

After generating risks, [Relate risks to each other](#) on page 96.

## Visualize and edit profile dependencies using the GRC Workbench

The GRC Workbench gives GRC administrators a graphical interface to create profile dependencies. These relationships enable consistent profile and risk mapping and modeling across the enterprise.

Role required: sn\_grc.manager

1. Navigate to Risk GRC Workbench .
2. Select the Model Setup tab at the top, then select the Dependency tab below it.
3. Search for and select a profile from the list on the left.  
Profiles are organized hierarchically by profile class, then by profile.
4. After selecting a profile from the left, the profile is displayed in the center with its direct upstream and downstream dependencies.  
On the right, eligible profiles that can be added as upstream or downstream dependencies are listed.
5. Perform one of the following actions:

Option	Description
<b>To add an upstream profile dependency</b>	Drag an eligible upstream profile from the list of eligible profiles on the right and drop it on the top half of the profile in the center of the page.
<b>To add a downstream profile dependency</b>	Drag an eligible downstream profile from the list of eligible profiles on the right and drop it on the bottom half of the profile in the center of the page.

The profiles are removed from the right menu when moved to the center of the page.

## Delete profile dependencies using the GRC Workbench

When deleting profile dependencies, only the relationship between the profiles is deleted. The profiles themselves remain unmodified.

Role required: admin

1. Navigate to Risk GRC Workbench .
2. Select the Model Setup tab at the top, then select the Dependency Map tab below it.
3. Search for and select the desired profile from the list on the left.  
After selecting a profile from the left, the profile is displayed in the center with its direct upstream and downstream dependencies.
4. In the center tree, point to the upstream or downstream risk that should be disassociated from the selected center risk. As you point to the risk, a delete icon appears, click the delete icon.
5. Click Delete in the confirmation dialog to confirm the deletion of the relationship.

---

**Note:** Only the relationship between the profiles is deleted. The profiles themselves remain unmodified.

---

## Delete a profile class using the GRC workbench

Deleting a profile class, deletes all of the relationships below it.

Role required: admin

1. Navigate to Risk GRC Workbench .
2. Select the Model Setup tab at the top, and select the Dependency Model tab below.
3. Select the desired profile class from the list on the left.  
After selecting a profile from the left, the profile is displayed in the center with its direct upstream and downstream dependencies.
4. Click the delete icon to the right of the profile class name.
5. In the deletion confirmation popup, click Delete.  
Deleting the profile class deletes all of the relationships below it.

## Create a risk using the GRC Workbench

Risk managers can create risks directly from the GRC workbench.

Role required: sn.\_risk.admin or sn.risk.manager

1. Navigate to Risk GRC Workbench .
2. Select the Risk Dependencies tab at the top, then select the Relationships tab below it.
3. On the left, in the Risks section, click Create Risk.
4. Fill in the fields on the form, as appropriate.

Table 31: Risk

Field	Description
Name	Enter a name for the risk. Field is auto-populated if the risk is generated from a risk statement, but can be changed without affecting the relationship between the risk and risk statement.
Number	Read-only field that is automatically populated with a unique identification number.
State	<p>The risk state is a read-only field. Possible choices are:</p> <ul style="list-style-type: none"> <li>• Draft In this state, all risk users can modify the risk. Only available when creating a one-off control. One-off controls are possible but not recommended.</li> <li>• Attest When the risk is created from a risk statement, controls are in this state.</li> </ul> <hr/> <p><b>Note:</b> When a risk is set back to draft, the assessment is canceled.</p> <hr/> <ul style="list-style-type: none"> <li>• Review Risks are automatically moved to review from the assessment phase.</li> <li>• Monitor In this state, all risk managers can move the risk from review to monitor.</li> <li>• Retired Risk managers or administrators can move a risk from Monitor to Retired. Indicators do not run when the risk is in this state.</li> </ul> <hr/> <p><b>Note:</b> When a risk is retired, any assessment associated with it is canceled.</p> <hr/>
Owning group	Select an owning group for the risk.

Field	Description
Category	<p>Choose a category of risk which applies to the profile.</p> <ul style="list-style-type: none"> <li>• Legal</li> <li>• Financial</li> <li>• Operational</li> <li>• Reputational</li> <li>• Legal/Regulatory</li> <li>• Credit</li> <li>• Market</li> <li>• IT</li> </ul> <p>Field is auto-populated if risk is generated from a risk statement.</p>
Owner	<p>Select an owner for the risk.</p> <hr/> <p><b>Note:</b> The owner is always added as a respondent.</p> <hr/>
Statement	Select the statement this risk is associated with.
Profile*	<p>Relate the risk to a specific profile.</p> <hr/> <p><b>Note:</b> Only active profiles are shown.</p> <hr/>
Description	Describe the Risk and how it is a threat to the organization.
Additional Information	Include any details which will help others understand the risk record.

---

**Note:** \* indicates a mandatory field.

---

5. Click the Assessment tab.
6. Fill in the fields on the form, as appropriate.

**Table 32: Risk Scoring**

Field	Description
Assessment	The assessment to attach to this risk.
Assessment respondents	<p>Users assigned to the assessment of this risk.</p> <hr/> <p><b>Note:</b> Only a user with the sn_grc.user role can be added as a respondent.</p> <hr/>

When both the Assessment and Assessment respondents fields are set, assessments are created when you click Assess.

7. Click the Scoring tab.
8. Fill in the fields on the form, as appropriate.

**Table 33: Risk Scoring**

Field	Description
Inherent SLE	Monetary value of a risk if it occurs before any mitigation strategies are in place.
Residual SLE	Monetary value of a risk if it occurs after all mitigation strategies are in place.
Inherent ARO	Probability that a risk will occur in any given year before any mitigation strategies are in place.
Residual ARO	Probability that a risk will occur in any given year after all mitigation strategies are in place.
Inherent ALE	Annualized loss expectancy ALE = SLE x ARO before any mitigation strategies are in place.
Residual ALE	Annualized loss expectancy ALE = SLE x ARO after all mitigation strategies are in place.
Inherent score	The score of the risk before any mitigation strategies are in place.
Residual score	The score of the risk after all mitigation strategies are in place.
Calculated ALE	Annualized loss expectancy based off all calculations.
Calculated score	The corresponding score for the calculated ALE.

9. Click the Response tab.
10. Fill in the fields on the form, as appropriate.

**Table 34: Risk Response**

Field	Description
Response	<ul style="list-style-type: none"> <li>• Accept</li> <li>• Avoid</li> <li>• Mitigate</li> <li>• Transfer</li> </ul>

Field	Description
Justification	Enter a reasonable justification for the selected response

- Click the Monitoring tab.

**Note:** The fields on the Risk Monitoring tab are read-only.

**Table 35: Risk Monitoring**

Field	Description
Control compliance	Percentage of compliant controls
Control non-compliance	Percentage of non-compliant controls
Control failure factor	Sum of failed controls weighting divided by total controls weighting
Indicator failure factor	Uses the last result of each associated indicator. Number of last results failed divided by total number of indicators associated.
Calculated risk factor	This value is calculated from (Indicator failure factor + Control failure factor) / 2.

- Click the Activity Journal tab.
- Enter additional comments, as necessary.
- Click Submit.

The risk is created and centered in the middle of the page. Additionally, the risk is selected on the right.

## Visualize and edit risk dependencies using the GRC Workbench

The GRC Workbench gives GRC administrators a graphical interface to create risk dependencies. These relationships enable consistent profile and risk mapping and modeling across the enterprise.

Role required: sn\_risk.manager

- Navigate to Risk GRC Workbench .
- Select the Risk Dependencies tab at the top, then select the Relationships tab below it.
- Search for and select a risk from the list on the left.  
Risks are organized hierarchically by profile class, then by profile.
- After selecting a risk from the left, the risk is displayed in the center with its direct upstream and downstream dependencies.  
On the right, eligible risks that can be added as upstream or downstream dependencies are listed.
- Perform one of the following actions:

Option	Description
<b>To add an upstream risk dependency</b>	Drag an eligible upstream risk from the list of eligible risks on the right and drop it on the top half of the risk in the center of the page.

Option	Description
To add a downstream risk dependency	Drag an eligible downstream risk from the list of eligible risks on the right and drop it on the bottom half of the risk in the center of the page.

## Delete risk dependencies using the GRC Workbench

When deleting risk dependencies, only the relationship between the risks is deleted. The risks themselves remain unmodified.

Role required: sn\_risk.manager

1. Navigate to Risk GRC Workbench .
2. Select the Risk Dependencies tab at the top, then select the Relationships tab below it.
3. Search for and select a risk from the list on the left.  
Risks are organized hierarchically by profile class, then by profile.
4. In the center tree, point to the upstream or downstream risk that should be disassociated from the selected center risk. As you point to the risk, a delete icon appears, click the delete icon.
5. Click Delete in the confirmation dialog to confirm the deletion of the relationship.

---

**Note:** Only the relationship between the risks is deleted. The risks themselves remain unmodified.

---

## Risk Library

The risk library contains all risk frameworks and risk statements. Risk frameworks are used to group risk statements into manageable categories, while risk statements group the individual risks.

### Create a risk statement

Risk managers create risk statements to group risks into manageable categories.

Role required: sn\_risk.manager

1. Navigate to Risk Risk Library Risk Statements .
2. Click New.
3. Fill in the fields on the form, as appropriate.

---

**Note:** When any of the following statement fields changes: Name, Description, Reference, Category, Type, Classification, and Attestation, all the associated controls and risks are updated, and their state is set back to Draft.

---

**Table 36: Risk Statement**

Field	Description
Name*	The name of the risk statement.
Framework	Select the framework this risk statement is associated with.



Field	Description
Category	Choose a category. <ul style="list-style-type: none"> <li>• Legal</li> <li>• Financial</li> <li>• Operational</li> <li>• Reputational</li> <li>• Legal/Regulatory</li> <li>• Credit</li> <li>• Market</li> <li>• IT</li> </ul>
Description	A description of the risk statement.
Additional information	Additional information for this risk statement.
Inherent impact	Select a number indicating how much impact the risk poses. <ul style="list-style-type: none"> <li>• 5 - Very High</li> <li>• 4 - High</li> <li>• 3 - Moderate</li> <li>• 2 - Low</li> <li>• 1 - Very Low</li> </ul>
Inherent likelihood	Select a number indicating the likelihood of the identified risk occurring. <ul style="list-style-type: none"> <li>• 5 - Extremely Likely</li> <li>• 4 - Likely</li> <li>• 3 - Neutral</li> <li>• 2 - Unlikely</li> <li>• 1 - Extremely Unlikely</li> </ul>
Residual impact	Select a number indicating how much impact the risk poses with all mitigation strategies in place <ul style="list-style-type: none"> <li>• 5 - Very High</li> <li>• 4 - High</li> <li>• 3 - Moderate</li> <li>• 2 - Low</li> <li>• 1 - Very Low</li> </ul>

Field	Description
Residual likelihood	<p>Select a number indicating the likelihood of the identified risk occurring with all mitigation strategies in place.</p> <ul style="list-style-type: none"> <li>• 5 - Extremely Likely</li> <li>• 4 - Likely</li> <li>• 3 - Neutral</li> <li>• 2 - Unlikely</li> <li>• 1 - Extremely Unlikely</li> </ul>

---

**Note:** Accurate default scoring selections are important for normalizing risk across the organization.

---

4. Click Submit.

## Create a risk framework

Risk managers create risk frameworks to group risk statements into manageable categories.

Role required: sn\_risk.manager

1. Navigate to Risk Risk Library Frameworks .
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 37: Risk Framework**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
Active	Check box that determines whether the risk framework is active.
Name*	The name of the risk framework.
Description	A description of the risk framework.
Additional information	Additional information for this risk framework.

4. Click Submit.
5. Select the risk framework from the list to reopen it.
6. In the Risk Statements Related List, select Edit to add the risk statements to the risk framework.
7. Click Save.

## GRC profile scoping

The Scoping module contains profiles and profile types for use in all GRC-related applications. They can be created for any record on any table.

The GRC: Profile plugin contains the Scoping module and is not visible to customers and requires activation of the Policy and Compliance Management plugin, the Risk Management plugin, or the Audit Management plugin.

Only one profile can exist for a record. That profile, however, can belong to many profile types. Profile types and profiles are used differently depending on the application:

- Risk managers use profile types and profiles to monitor risk exposure and perform risk assessments.
- Policy and compliance managers use profile types and profiles to create a system of internal controls and monitor compliance.

### Profiles

Profiles are the records that aggregate GRC information related to a specific item. Each profile is associated with a single record from any table in the application. Profiles cannot be created for items that do not have a record in a table in the platform.

### Profile Classes

Profile classes allow GRC managers to separate profiles for better distinction. For example, Business Service Profiles, Department Profiles, Business Unit Profiles, and the like.

### Profile Types

Profiles types are dynamic categories containing one or more profiles. Business logic automates the process of creating and categorizing any profiles in the system that meet the profile type conditions. Profile types are assigned to policy statements, which generate controls for every profile listed in the profile type.

## Create and edit a profile type

Administrators or managers in any of the GRC-related applications, create profiles types from which profiles are generated.

Role required: sn\_compliance.admin or sn\_compliance.manager, sn\_risk.admin or sn\_risk.manager, sn\_audit.admin or sn\_audit.manager

1. Navigate to one of the following locations:
  - Audit Scoping Profile Types .
  - Policy and Compliance Scoping Profile Types .
  - Risk Scoping Profile Types .

2. Do one of the following actions:

Option	Description
<b>To create a new profile type</b>	Click New.
<b>To edit a profile type</b>	Open the profile type.

3. Fill in the fields on the form, as appropriate.

Table 38: Profile type

Name	Description
Name*	The name of the profile type.
Description	An explanation of the profile type with any additional information about the profile type that a user will find helpful.
Table*	The table from which the profile type conditions identify the records to create profiles.
Condition	Filter conditions to restrict which profiles belong to a specific profile type.
Use owner field	Select the check box to indicate that a default owner field should be used when generating new profiles.
Default owner	The field on the table specifying the person who owns any new profiles generated from the profile type.
Default profile class	<p>Set the default profile class.</p> <p>Generated profiles copy this default profile class under the following conditions:</p> <ul style="list-style-type: none"> <li>• when the profile's class is empty and it's associated to a profile type that has a default profile class</li> <li>• when a profile is created under a profile type that has a default profile class</li> </ul> <p>The existing profile's class is updated under the following conditions:</p> <ul style="list-style-type: none"> <li>• The profile type's table changes</li> <li>• The profile type's condition changes</li> <li>• The profile type's active field is ik;8,'</li> <li>• The profile type's default profile class changes</li> </ul>

---

**Note:** \* indicates a mandatory field.

---

4. Click Submit.

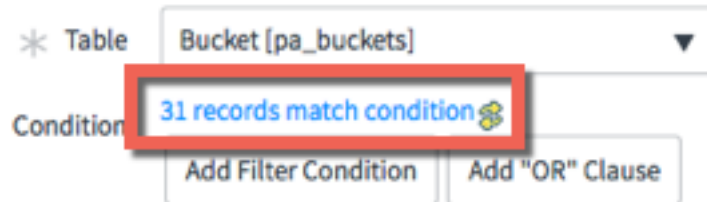
## Generate a profile from a profile type

Profiles are generated automatically from profile types in any of the GRC-related applications.

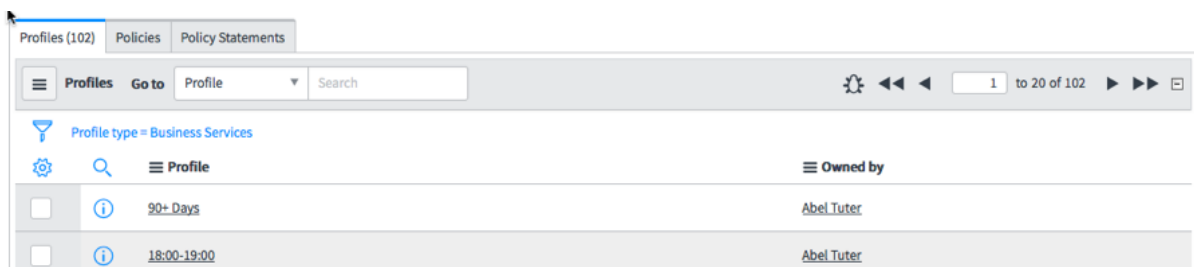
Role required: sn\_compliance.admin or sn\_compliance.manager, sn\_risk.admin or sn\_risk.manager, sn\_audit.admin or sn\_audit.manager

1. Navigate to one of the following locations:
  - Audit Scoping Profile Types
  - Policy and Compliance Scoping Profile Types
  - Risk Scoping Profile Types
2. Open the Profile Type record.
3. Add or modify any conditions, as necessary.

Changing the Table, changes the number of records matching the condition.



4. Assign the Owner field.
  5. Click Update.
- A profile is generated for every record that matches the filter condition.



## Deactivate a profile

When a profile is deactivated, all the controls related to that profile are retired, and the indicators and test plans associated to those controls are marked in-active.

Role required: grc\_manager

The owner of the profile can edit the profile record and deactivate it.

1. Navigate to one of the following locations:
  - Audit Scoping All Profiles
  - Policy and Compliance Scoping All Profiles
  - Risk Scoping All Profiles

2. Open the profile record.
  - If the Active check box is selected, then the profile is active.
  - If the Active check box is not selected, then the profile is inactive.
3. Click Update.
  - All associated controls change to the retired state.
  - All the indicators and test plans associated with the retired control are marked in-active.

## Reactivate a profile

When a profile is reactivated, associated controls and risks return to the draft state and the indicators and test plans return to active.

Role required: grc\_manager

The owner of the profile can edit the profile record and reactivate it.

1. Navigate to one of the following locations:
  - Audit Scoping All Profiles
  - Policy and Compliance Scoping All Profiles
  - Risk Scoping All Profiles
2. Open the profile record.
3. In the profile, select the check box marked Active.
4. Click Update.
 

All associated controls, risks, indicators, and test plans are also re-activated or retired.

## Create a profile class

GRC managers create profile classes representing the types of things that will be part of the dependency model. Reports can be filtered to define relationships between the different profile classes. A profile class defines what a profile actually is. It differs from a profile type (for example, Business Services and Critical Business Services), in that a profile can belong to many profile types but a profile can have only one profile class (for example, Business Service).

Role required: sn\_grc.manager

1. Navigate to one of the following locations:
  - Audit Scoping Profile Classes
  - Policy and Compliance Scoping Profile Classes
  - Risk Scoping Profile Classes
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 39: Authority Document**

Field	Value
Name	Name of the profile class.

Field	Value
Roll up to	Select dependencies to other profiles. Useful for reporting how your lower-level operational risks impact corporate-level risks.
Is Root	Select the check box to indicate that this is the highest level class.  <b>Note:</b> Only one root class is allowed and it cannot roll up to another class.

4. Click Submit.

## Assign profiles to classes

GRC managers assign profiles to classes for the filtering of reports and to define relationships between the different classes of business services.

Role required: sn\_compliance.manager

1. Navigate to one of the following locations:
  - Audit Scoping All Profiles
  - Policy and Compliance Scoping All Profiles
  - Risk Scoping All Profiles
2. Open the profile record.
3. Assign the Class.
4. Click Update.

## Risk Register

The risk register is the central repository for all potential risks that could occur at anytime, anywhere in the organization.

Risks are generated from risk frameworks, risk statements, and profiles, or they are created manually.

## Associate a risk framework or risk statement with a profile type to generate risks

Making associations between risk frameworks or risk statements and profile types automatically generates risks.

Role required: sn\_risk.admin and sn\_risk.manager

1. Navigate to Risk Scoping Profile types .
2. Open the profile type record.
3. In the Risk Framework or Risk Statement related list, click Edit.
4. Select the risk frameworks or risk statements to associate to the profile, and click Save.

All risk frameworks (or risk statements) are associated to the profile type and a risk is created for every risk statement against every profile in the profile type.

## Generate a risk from a risk framework

Making associations with risk frameworks automatically creates risks.

Role required: sn\_risk.admin and sn\_risk.manager

1. Navigate to Risk Risk Library Risk Framework .
2. Open the risk framework record.
3. In the Profile Type Related List, click Edit.
4. Select the profile types to associate to the risk framework, and click Save.  
All risk statements are associated to the profile type and a risk is created for every risk statement against every profile in the profile type.

## Generate a risk from a risk statement

Making associations with risk statements automatically creates risks.

Role required: sn\_risk.admin and sn\_risk.manager

1. Navigate to Risk Risk Library Risk Statement .
2. Open the risk statement record.
3. In the Profile Type Related List, click Edit.
4. Select the profile types to associate to the risk statement, and click Save.  
One risk is generated for each profile in the profile type based on the risk statement.

## Relate risks to each other

Create relationships between risks to better understand how risks affect each other and how they affect the enterprise.

Role required: sn\_risk.manager or sn\_risk.admin

1. Navigate to Risk Risk Register All Risks .
2. Open a risk.
3. Perform one of the following actions:

Option	Description
<b>To specify that the current risk is downstream of another risk</b>	Click the Add button in the Upstream Risks related list.
<b>To specify that the current risk is upstream of another risk</b>	Click the Add button in the Downstream Risks related list

4. Select the desired risks to relate to the current risk and click Create Relationship.

## Create a risk manually

Risk administrators can create risk records when they see a potential for a gain or loss of value.



Role required: sn\_risk.admin and sn\_risk.manager

1. Navigate to Risk Risk Register Create New .
2. Fill in the fields on the form, as appropriate.

**Table 40: Risk**

Field	Description
Name	Enter a name for the risk. Field is auto-populated if the risk is generated from a risk statement, but can be changed without affecting the relationship between the risk and risk statement.
Number	Read-only field that is automatically populated with a unique identification number.
State	<p>The risk state is a read-only field. Possible choices are:</p> <ul style="list-style-type: none"> <li>• <b>Draft</b> In this state, all risk users can modify the risk. Only available when creating a one-off control. One-off controls are possible but not recommended.</li> <li>• <b>Attest</b> When the risk is created from a risk statement, controls are in this state.</li> </ul> <hr/> <p><b>Note:</b> When a risk is set back to draft, the assessment is canceled.</p> <hr/> <ul style="list-style-type: none"> <li>• <b>Review</b> Risks are automatically moved to review from the assessment phase.</li> <li>• <b>Monitor</b> In this state, all risk managers can move the risk from review to monitor.</li> <li>• <b>Retired</b> Risk managers or administrators can move a risk from Monitor to Retired. Indicators do not run when the risk is in this state.</li> </ul> <hr/> <p><b>Note:</b> When a risk is retired, any assessment associated with it is canceled.</p> <hr/>
Owning group	Select an owning group for the risk.

Field	Description
Category	<p>Choose a category of risk which applies to the profile.</p> <ul style="list-style-type: none"> <li>• Legal</li> <li>• Financial</li> <li>• Operational</li> <li>• Reputational</li> <li>• Legal/Regulatory</li> <li>• Credit</li> <li>• Market</li> <li>• IT</li> </ul> <p>Field is auto-populated if risk is generated from a risk statement.</p>
Owner	<p>Select an owner for the risk.</p> <hr/> <p><b>Note:</b> The owner is always added as a respondent.</p> <hr/>
Statement	Select the statement this risk is associated with.
Profile*	<p>Relate the risk to a specific profile.</p> <hr/> <p><b>Note:</b> Only active profiles are shown.</p> <hr/>
Description	Describe the Risk and how it is a threat to the organization.
Additional Information	Include any details which will help others understand the risk record.

---

**Note:** \* indicates a mandatory field.

---

3. Click the Assessment tab.
4. Fill in the fields on the form, as appropriate.

**Table 41: Risk Scoring**

Field	Description
Assessment	The assessment to attach to this risk.
Assessment respondents	<p>Users assigned to the assessment of this risk.</p> <hr/> <p><b>Note:</b> Only a user with the sn_grc.user role can be added as a respondent.</p> <hr/>

When both the Assessment and Assessment respondents fields are set, assessments are created when you click Assess.

5. Click the Scoring tab.
6. Fill in the fields on the form, as appropriate.

**Table 42: Risk Scoring**

Field	Description
Inherent SLE	Monetary value of a risk if it occurs before any mitigation strategies are in place.
Residual SLE	Monetary value of a risk if it occurs after all mitigation strategies are in place.
Inherent ARO	Probability that a risk will occur in any given year before any mitigation strategies are in place.
Residual ARO	Probability that a risk will occur in any given year after all mitigation strategies are in place.
Inherent ALE	Annualized loss expectancy ALE = SLE x ARO before any mitigation strategies are in place.
Residual ALE	Annualized loss expectancy ALE = SLE x ARO after all mitigation strategies are in place.
Inherent score	The score of the risk before any mitigation strategies are in place.
Residual score	The score of the risk after all mitigation strategies are in place.
Calculated ALE	Annualized loss expectancy based off all calculations.
Calculated score	The corresponding score for the calculated ALE.

7. Click the Response tab.
8. Fill in the fields on the form, as appropriate.

**Table 43: Risk Response**

Field	Description
Response	<ul style="list-style-type: none"> <li>• Accept</li> <li>• Avoid</li> <li>• Mitigate</li> <li>• Transfer</li> </ul>

Field	Description
Justification	Enter a reasonable justification for the selected response

- Click the Monitoring tab.

**Note:** The fields on the Risk Monitoring tab are read-only.

**Table 44: Risk Monitoring**

Field	Description
Control compliance	Percentage of compliant controls
Control non-compliance	Percentage of non-compliant controls
Control failure factor	Sum of failed controls weighting divided by total controls weighting
Indicator failure factor	Uses the last result of each associated indicator. Number of last results failed divided by total number of indicators associated.
Calculated risk factor	This value is calculated from (Indicator failure factor + Control failure factor) / 2.

- Click the Activity Journal tab.
- Enter additional comments, as necessary.
- Click Submit.

## Follow a risk

Connect integrates with Risk Management providing an overlay to the standard interface, allowing users to participate in conversations while they work and collaborate on the risk record.

Role required: sn\_risk.user

For more information about Connect, see [Connect](#).

- Navigate to Risk Risk Register All Risks .
- Open the risk record.
- Click the Follow tab and perform one of the following actions:

Option	Action
<b>To add the Connect sidebar</b>	<ul style="list-style-type: none"> <li>Click Open Connect mini.</li> </ul>
<b>To add the Connect full-screen view</b>	<ul style="list-style-type: none"> <li>Click Open Connect Full.</li> </ul>

## Add an indicator to a risk

When adding indicators to a risk, templates must be associated to the risk statements.

Role required: sn\_risk.admin and sn\_risk.manager

1. Navigate to Risk Risk Register All Risks .
2. Open the risk record.
3. Continue with one of the following options.

Option	Description
<b>Select an indicator from the indicator templates</b>	<ol style="list-style-type: none"> <li>1. In the Indicators Related List, click Add.</li> <li>2. Select the indicator templates to associate to the risk.</li> <li>3. Click Save.</li> </ol>
<b>Add a new indicator</b>	<ol style="list-style-type: none"> <li>1. In the Indicators Related List, click New.</li> <li>2. Fill in the fields on the form, as appropriate.</li> <li>3. Click Submit.</li> </ol>

All indicators are associated to the risk.

## Add a control to a risk

Controls are added to risks for the on-going review of processes.

Role required: sn\_risk.admin and sn\_risk.manager

1. Navigate to Risk Risk Register All Risks
2. Open the risk record.
3. Continue with one of the following options.

Option	Description
<b>Add an existing control</b>	<ol style="list-style-type: none"> <li>1. In the Controls related list, click Add.</li> <li>2. Select the controls that are associated with the risk profile.</li> <li>3. Click Add relationship.</li> </ol> <p><b>Note:</b> The controls displayed after clicking the Add relationship button are limited to controls that have the same profile as the current risk. If there are no eligible controls that can be related to the risk, the Add button is not displayed on the Controls related list.</p>
<b>Add a new control</b>	<ol style="list-style-type: none"> <li>1. In the Controls Related List, click New.</li> <li>2. Fill in the fields on the form, as appropriate.</li> <li>3. Click Submit.</li> </ol>

## Risk assessments

Assessments are surveys that gather evidence to determine risk. Risks start in a Draft state then move to Assess, which sends a notification to the Assessment respondents.

By default, GRC Assessment is used for risks and provides the following assessment questions:

- Is this control implemented?
- Attach evidence
- Explain

My Assessments is contained in the Risk Register module and contains active assessments for which you are the respondent. The assessments appear in a list with a single assessments record per risk.

All Assessments is contained in the Risk Register module and contains all active assessments. The assessments appear in a list with a single assessments record per risk.

Compliance managers can create a new set of questions for each policy statement. See .

## Assess a risk

Risks start in a Draft state then move to Assess, which sends a notification to the Assessment respondents.

Role required: sn\_grc.user

Risk assessments do not appear in the Self-Service My assessments & surveys module, because hundreds of GRC assessment records could be generated at once and should be separated from other assessments, in a separate list view.

1. Navigate to Policy and Compliance Controls My Attestations .
2. Open the attestation and review the details.

Option	Description
<b>If you are unable to answer the questions</b>	<ol style="list-style-type: none"> <li>1. Reassign the attestation to another user in the Assigned to field.</li> <li>2. Click Update and close the record.</li> </ol> <p style="text-align: right;"><b>Note:</b> Only a user with the sn_grc.user role can be re- assigned the assessment.</p> <p>The list of attestations refreshes when you reassign an attestation to another user.</p>
<b>If you are able to answer the questions</b>	<ol style="list-style-type: none"> <li>1. Click Take assessment.</li> <li>2. Answer the questions and attach information, as required.</li> <li>3. Click Submit.</li> </ol> <p>The list of attestations refreshes when you close the Take Assessment pop-up window.</p>

## Create an assessment type

The risk manager can create a new set of questions for each risk assessment.

Role required: sn\_risk.asmt\_creator or sn\_risk.manager or sn\_risk.administrator

1. Navigate to Risk Administration Assessment Types .
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 45: Assessment Metric Type**

Field	Description
Name	The name of the assessment type.
Assessment duration	
Table	
Scale factor	
Condition	
Description	
State	
Enforce condition	
Roles	

4. Click Submit.

## Risk assessment designer

The risk assessment designer provides a single interface that users can use to create, edit, and distribute assessment, as well as change scoring parameters.

All assessment records are stored in assessment tables and displayed in assessment views of those tables.

The designer contains the following elements:

**Table 46: Elements of the Assessment Designer**

Element	Description
Controls	Controls for the supported question data types are available in the Controls palette. Drag a control onto the designer canvas to create a question of that type.
Header bar	The header bar contains tabs that display different views and a menu of various functions. The availability of each option depends on the status of the assessment that is opened in the designer.
Design canvas	New assessments open in the Design view. The assessment Name field appears above the first category in the canvas. A blank question field appears in the category container.

*Create an assessment using the assessment designer*

The assessment designer includes a design canvas, a header bar, and many controls for creating assessments.

Role required: sn\_compliance.attest\_creator, sn\_compliance.manager, sn\_compliance.administrator

1. Navigate to Risk Administration Assessment Types .
2. Click Assessment Designer.  
The designer contains the following elements:
  - Controls
  - Header bar
  - Design canvas
3. Enter a name in the Name field above first category in the canvas.  
A blank question field appears in the category container.
4. Drag a control onto the designer canvas to create a question of that type.

**Table 47: Question controls**

Data type	Description	Scored
Attachment	Question with a Manage Attachments icon that allows users to attach one or more files.	Y
Boolean	Question with a check box or a Yes/No list for user responses.	
Choice	List of predefined options. For more information, see the definition for Choices.	Y
Date	Date field.	N
Date/Time	Date and time field.	N
Number	Number field with predefined minimum and maximum values. The default is 1-10.	N
Percentage	Percentage field with a prescribed range.	N
Scale	Predefined <i>Likert scale</i> . Answer options appear as radio buttons.	Y
Numeric Scale	Selectable number scale. The default is 1-5. Answer options appear as radio buttons.	Y
String	Single or multi-line text field.	N
Template	Choice list of templates that provide a predefined scale of options. .	Y



Data type	Description	Scored
Reference	Choice list of fields from a specified reference table. This data type does not support reference qualifiers.	

5. Click one of the following tabs to change the view in the canvas:

Option	Description
<b>Design</b>	Add categories and questions, and configure the properties of each. This is the default view of the canvas when you open the designer.
<b>Configuration</b>	Create introductions and end notes for assessments, and select a signature.
<b>Availability</b>	Select the recipients for each category in the assessment.

6. Point to the menu icon in the upper right of the Assessment Designer to select one of the following options:

**Note:** The availability of each option depends on the status of the a that is opened in the designer.

Option	Description
<b>Save</b>	Save the current assessment.
<b>Preview</b>	Display a preview to the selected recipients.
<b>Publish</b>	Distributes the assessment to the selected recipients.
<b>Save and Publish</b>	Saves and distributes the assessment in one step.
<b>New Attestation</b>	Opens a fresh canvas for a new assessment.
<b>Load Attestation</b>	Opens a list of existing assessment that you can select and edit.

## GRC issues management

Issues can be created manually to document audit observations, remediations, or to accept any problems. They are automatically generated from indicator results, attestation results, or control test effectiveness.

An issue is created automatically when:

- Issue - An indicator fails
- Control issue - A control attestation is completed indicating that the control is Not implemented
- Control test issue - A control test is closed complete with the control effectiveness set to Ineffective
- Other issue - is created by the user manually

Remediating an issue marks an intention to fix the underlying issue causing the control failure or risk exposure. Accepting an issue marks an intention to create an exception for a known control failure or risk.

Controls that are Accepted remain in a non-compliant state until the control is reassessed. In this way, the issue can be used to document observations during audits.

## Create a GRC issue manually

Manually create issues to document audit observations, the intention of remediations, or to accept any problems.

Role required: (per product)

- In GRC: compliance\_admin, compliance\_manager, or sn\_compliance.user
- In Risk Management: \_admin, risk\_manager, or sn\_risk.user
- In Audit Management: audit\_admin, audit\_manager, or audit\_admin or sn\_audit.user

1. Navigate to one of the following locations:
  - Audit Issues Create New .
  - Policy and Compliance Issues Create New .
  - Risk Issues Create New .
2. Fill in the fields on the form, as appropriate.

**Table 48: Issue**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
State	<ul style="list-style-type: none"> <li>• New</li> <li>• Analyze</li> <li>• Respond</li> <li>• Review</li> <li>• Closed</li> </ul>
Assignment group	A group assigned to the issue.
Assigned to	The user assigned to the issue.
Priority	Priority for this issue: <ul style="list-style-type: none"> <li>• 1 - Critical</li> <li>• 2 - High</li> <li>• 3 - Moderate</li> <li>• 4 - Low</li> <li>• 5 - Planning</li> </ul>
Short description	Brief description of the issue.
Details	
Profile	The related profile.
Item	The related control or risk.
Description	A more detailed explanation of the issue.

Field	Description
Recommendation	The recommended action to resolve this issue.
Dates	
Planned start date	Date and time that work on the issue is expected to begin.
Planned end date	Date and time that work on the issue is expected to end.
Planned duration	Estimated amount of work time. Calculated using the Planned start date and Planned end date.
Actual start date	Time when work began on this issue
Actual end date	Time when work on this issue was completed.
Actual duration	Amount of work time. Calculated using the Actual start date and Actual end date.
Activity	
Work notes	Information about how to resolve the issue, or steps already taken to resolve it, if applicable. Work notes are visible to users who are assigned to the issue.
Additional comments (Customer visible)	Public information about the enhancement request.
Engagement	
Engagement	The related engagement.

3. Click Submit.

## GRC continuous monitoring

Continuous monitoring involves activities related to identifying and creating key risk and controls indicators. Supporting information can be collected for those indicators through automatic data collection or manual tasks. Indicator results are then used to create issues for controls, update risk scores, and provide supporting information for audit activities and control testing.

### Indicators

Indicators collect data to monitor controls and risks, and collect audit evidence. Indicators monitor a single control or risk.

### Indicator templates

Indicator templates allow the creation of multiple indicators for similar controls or risks.

## Create a GRC indicator

Indicator data for controls, risk, and audit evidence are measured differently depending on the GRC-related application.

Role required: compliance\_admin or compliance\_manager, risk\_admin or risk\_manager, audit\_admin or audit\_manager

1. Navigate to one of the following locations:
  - Policy and Compliance Indicators Indicators .
  - Risk Indicators Indicators .
  - Audit Indicators Indicators .
2. Select New.
3. Fill in the fields on the form, as appropriate.

**Table 49: Indicator**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
Active	Check box that determines whether the indicator is active.
Name	Name of the indicator.
Item	The related control or risk.
Template	The related indicator template.
Applies to	The profile related to the Item.
Owner	The indicator owner.
Owning group	The group that owns the indicator.
Override Template	Click to override the indicator template associated to this indicator
Last result passed	Read-only field indicating whether last result passed.
Schedule	
Collection frequency	Select the collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule.
Next run time	Read-only field that is automatically populated with the next collection time for indicator results.
Method	

Field	Description
Type	Results can be gathered manually using task assignment or automatically using basic filter conditions, Performance Analytics, or a script. <ul style="list-style-type: none"> <li>• Manual</li> <li>• Basic</li> <li>• Script</li> </ul>
Short Description	If Type is Manual, this field is present. Brief description of the issue.
Instructions	If Type is Manual, this field is present. Instructions for the collection of indicator results.
Value Mandatory	If Type is Manual, this field is present.
Passed/Failed	If Type is Basic, this field is present. Indicator passes or fails.
PA Threshold	If Type is PA Indicator, this field is present. The associated PA Threshold.
Script	If Type is Script, this field is present. Script that obtains the desired system information.
Supporting Data	
Table	Use supporting data to gather supporting evidence from other applications.
Supporting data fields	Supporting data fields based on the selected table.

4. Click Submit.

## Create a GRC indicator template

Compliance or risk managers create indicator templates from which many indicators can be created.

Role required: compliance\_admin or compliance\_manager, risk\_admin or risk\_manager, audit\_admin or audit\_manager

1. Navigate to one of the following locations:
  - Policy and Compliance Indicators Indicator Templates .
  - Risk Indicators Indicator Templates .
  - Audit Indicators Indicator Templates .
2. Select New.
3. Fill in the fields on the form, as appropriate.

Table 50: Indicator template

Field	Description
Name	Name of the indicator.
Active	Check box that determines whether the indicator template is active.
Content	The related policy or risk statement.
Schedule	
Collection frequency	Select the collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule.
Next run time	Read-only field that is automatically populated with the next collection time for indicator results.
Method	
Type	Results can be gathered manually using task assignment or automatically using basic filter conditions, Performance Analytics, or a script. <ul style="list-style-type: none"> <li>• Manual</li> <li>• Basic</li> <li>• PA Indicator</li> <li>• Script</li> </ul>
Short Description	If Type is Manual, this field is present. Brief description of the issue.
Instructions	If Type is Manual, this field is present. Instructions for the collection of indicator results.
Value Mandatory	If Type is Manual, this field is present.
Passed/Failed	If Type is Basic, this field is present. Indicator passes or fails.
PA Threshold	If Type is PA Indicator, this field is present. The associated PA Threshold.
Script	If Type is Script, this field is present. Script that obtains the desired system information.
Supporting Data	
Collect Supporting Data	Check to gather supporting evidence from other applications.

4. Click Submit.

## GRC PA Indicators

GRC PA Indicators link GRC content and items to Performance Analytics indicators, breakdowns and thresholds. You can associate Performance Analytics indicators with risk statements, risks, policy statements, and controls to view scorecards and trends and analyze current conditions and trends.

The risks and controls associated with a PA indicator or PA indicator/breakdown/element automatically monitor any PA threshold with the same PA indicator or PA indicator, breakdown, or element relationship. Any PA threshold breach is reported at the risk or control and Performance Analytics indicators relationship level within a breach counter. See [Performance Analytics](#).

### PA threshold breach impact

When a risk or control and Performance Analytics indicators relationship breach counter is different than zero (for example, a PA threshold with the same PA indicator or PA indicator, breakdown, or element relationship has breached), and if no opened issue already exists, then an issue is created which is associated to the risk or control. Additionally for risks, the Indicator failure factor represents the number of risk and Performance Analytics indicators relationships with a breach counter different than zero.

### Reset all PA Indicator breach counters

Reset breach counters associated to a risk or control by clicking Reset all PA Indicator breach counters or opening the specific relationship and clicking Reset Breach Counter.

### GRC PA indicator breach reports

There are two reports for the reporting of breaches:

- Risk PA Indicator Breaches
- Control PA Indicator Breaches

### Upgrade from Helsinki to Istanbul

After upgrading an instance from Helsinki to Istanbul, activate the GRC: Performance Analytics Premium Integration plugin. After doing so, every GRC indicator of type pa\_Indicator is migrated to the new GRC PA Integration and de-activated. The GRC indicators of type pa\_indicator is deactivated to avoid duplicate PA threshold events. If you prefer to continue using the GRC Indicator of type pa\_indicator, activate them again and deactivate the GRC PA Integration records that were created during the migration.

The trend in the PA indicator relationship shows only when the PA indicator has the Publish on Scorecards flag on. Otherwise no score is always displayed.

## Activate GRC: Performance Analytics Premium Integration

The GRC: Performance Analytics Premium Integration plugin provides an integration between Performance Analytics and the Risk Management and Policy and Compliance Management applications, providing more insight into organizational risk and compliance performance.

Role required: admin

This plugin includes demo data and activates related plugins if they are not already active.

1. Navigate to System Definition Plugins .
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

If the plugin has optional features that are not functional because other plugins are inactive, those plugins are listed. A warning states that some files are not installed. If you want the optional features to be installed, cancel this activation, activate the necessary plugins, and then return to activating the plugin.

4. If available, select the Load demo data check box.

Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.

5. Click Activate.

After activating the GRC: Performance Analytics Premium Integration plugin on an instance with customized related lists on content (risk or policy statement) or items (risk or control), you may have to manually add the PA Indicator to content relationships and/or the PA indicator to item relationships.

## Associate a Performance Analytics indicator with GRC content

You can associate Performance Analytics indicators with risk statements and policy statements to analyze trends related to the risk or policy.

Role required: sn\_risk.manager or sn\_compliance.manager

1. Navigate to one of the following locations:
  - Policy and Compliance Policies and Procedures Policy Statements .
  - Risk Risk Library Risk Statements .
2. Open a risk statement or policy statement.
3. In the PA Indicators related list, click New.
4. Fill in the fields on the form, as appropriate.

**Table 51: PA Indicators**

Field	Description
PA Indicator*	The performance analytics indicator to associate the Risk Statement or Policy Statement with.

5. Click Submit.

On the risk statement or policy statement form, in the PA Indicators related list, you see the associated indicator. You can optionally click View Indicator on the desired indicator to see the indicator's Performance Analytics scorecard. The PA Indicator associations are carried over to all risks or controls associated to the original risk statement or policy statement. Additionally, if the indicator has a breakdown that matches the risk or control's profile (for example a Business Service breakdown), the Breakdown and Element fields for the relationship are automatically filled in.



## Associate a Performance Analytics indicator with a GRC item

You can associate Performance Analytics indicators with risks and controls to analyze trends related to the profile that risk or control belongs to.

Role required: sn\_risk.manager or sn\_compliance.manager

1. Navigate to one of the following locations:
  - Policy and Compliance Controls All Controls .
  - Risk Risk Register All Risks .
2. Open a risk or control.
3. In the PA Indicators related list, click New.
4. Fill in the fields on the form, as appropriate.

**Table 52: PA Indicators**

Field	Description
PA Indicator*	The performance analytics indicator to associate the Risk or Control with.
Breakdown	Select a breakdown to view a specific trend based on the breakdown element.
Element	<p>Select the breakdown element to view a particular trend and scorecard.</p> <hr/> <p><b>Note:</b> This field is dependent on the Breakdown field is populated. When visible, it is mandatory.</p> <hr/> <p>Note: This field is only visible if the Breakdown field is populated. It is mandatory when visible</p>

5. Click Submit.
 

On the Risk or Control form, in the PA Indicators related list, you see the associated indicator. You can optionally click View Indicator on the desired indicator to see the indicator's Performance Analytics scorecard.

## Update associated GRC indicators for a set of items

You can update all of the items belonging to a GRC content record so each item is individually related to the PA indicator.

Role required: sn\_risk.manager or sn\_compliance.manager

1. Navigate to one of the following locations:
  - Policy and Compliance Policies and Procedures Policy Statements .
  - Risk Risk Library Risk Statements .
2. Open a Risk Statement or Policy Statement that has an associated Performance Analytics Indicator.
3. Click the Update PA Relationships related link.

All of the risks or controls related to the risk statement or policy statement are automatically associated with all of the risk statement or policy statement's indicators. Additionally, if the indicator has a breakdown that matches the risk or control's profile (for example a Business Service breakdown), the Breakdown and Element fields for the relationship are automatically filled in.

## Risk Management Administration

The Risk Management application provides properties associated with significance, likelihood, and application.

### Risk Criteria

Risk Criteria are the scoring values attributed to the likelihood that a risk will occur, and the impact to your organization if the risk does occur.

Risk criteria thresholds define a high/likely or low/unlikely score as shown:

**Table 53: Risk Criteria Thresholds**

Likelihood	Significance	Scores
1 = Extremely Unlikely	1 = Very Low	0-5 = Very Low
2 = Unlikely	2 = Low	6-10 = Low
3 = Neutral	3 = Moderate	11-15 = Moderate
4 = Likely	4 = High	16-20 = High
5 = Extremely Likely	5 = Very High	21-25 = Very High

**Table 54: Risk properties**

Name	Description
Maximum value for Significance	Sets the maximum value (1-10) for significance on the risk criteria table. Decimals cannot be used, and are rounded if input.
Maximum value for Likelihood	Sets the maximum value (1-10) for likelihood on the risk criteria table. Decimals cannot be used, and are rounded if input.
A list of tables that are available in the Applies to field on forms	If this field is blank, all tables are available on the various forms for Profile Types, Profiles, and Risks. Defines a comma-separated list of tables that are available in the Applies to field on the Profile Type, Profile, and Risk form. Add .extended after the table name to include all extended tables.

## Assessment Types

Risk managers can create a new set of questions for each risk assessment. See [Create an assessment type](#) on page 102.

## Audit Management

The ServiceNow® Audit Management application involves a set of activities related to planning audit engagements, executing engagements, and reporting findings to the audit committee and executive board. Engagement reporting assures key stakeholders that the organization's risk and compliance management strategy is effective.

The GRC: Audit Management (com.sn\_compliance) plugin is available as a separate subscription and requires activation.

### Explore

- [GRC Common Release notes](#)
- [Audit Management Release notes](#)
- [Upgrade to Istanbul](#)

### Set up

- [Activate Audit Management](#) on page 115

### Administer

- [Engagement Overview](#) on page 123
- [Audit Management Administration](#) on page 150

### Use

- [GRC profile scoping](#) on page 31
- [Engagement Workbench](#) on page 125
- [Audit testing](#) on page 143

### Develop

- [Developer training](#)
- [Developer documentation](#)
- [Components installed with Audit Management](#) on page 116

### Troubleshoot and get help

- [Ask or answer questions in the GRC community](#)
- [Search the HI Knowledge Base for known error articles](#)
- [Contact ServiceNow Support](#)

## Activate Audit Management

The GRC: Audit Management (com.sn\_audit) plugin is available as a separate subscription.

Role required: admin

This plugin includes demo data and activates related plugins if they are not already active.

1. Navigate to System Definition Plugins .
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

If the plugin has optional features that are not functional because other plugins are inactive, those plugins are listed. A warning states that some files are not installed. If you want the optional features to be installed, cancel this activation, activate the necessary plugins, and then return to activating the plugin.

4. If available, select the Load demo data check box.

Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.

5. Click Activate.

## Components installed with Audit Management

Activating the GRC: Audit Management (com.sn\_audit) plugin adds or modifies several tables, user roles, and other components.

### Tables installed with Audit Management

GRC: Audit Management adds the following tables.

Table	Description
Activity [sn_audit_activity]	Extends Audit Task [sn_audit_task] and stores audit activities
Audit Task [sn_audit_task]	Extends Planned Task [planned_task] and is a generic table for all tasks associated with an audit
Base Audit Test [sn_audit_base_test]	Base table for Test Templates and Test Plans
Control Test [sn_audit_control_test]	Extends Audit Task [sn_audit_task] and stores control tests
Control to Engagement [sn_audit_m2m_control_engagement]	Stores many-to-many relationships between controls and engagements
Engagement [sn_audit_engagement]	Extends Planned Task [planned_task] and stores engagements
Interview [sn_audit_interview]	Extends Audit Task [sn_audit_task] and stores interviews
Profile to Engagement [sn_audit_m2m_profile_engagement]	Stores many-to-many relationships between profiles and engagements
Risk to Engagement [sn_audit_m2m_risk_engagement]	Stores many-to-many relationships between risks and engagements
Test Plan [sn_audit_test_plan]	Extends Base Audit Test [sn_audit_base_test] and stores test plans
Test plan to Engagement [sn_audit_m2m_test_plan_engagement]	Stores many-to-many relationships between test plans and engagements
Test Template [sn_audit_test_template]	Extends Base Audit Test [sn_audit_base_test] and stores test templates

Table	Description
Walkthrough [sn_audit_walkthrough]	Extends Audit Task [sn_audit_task] and stores walkthroughs

**Note:** All additional tables installed by the dependent plugins are also needed for GRC: Audit Management.

## Properties installed with Audit Management

GRC: Audit Management adds the following properties.

Name	Description
Defines the workflow that will be used for control test approval sn_audit.control_test_approval_workflow	<ul style="list-style-type: none"> <li>Type: string</li> <li>Default value: Control Test Approval</li> </ul>
Defines the workflow that will be used for engagement approval sn_audit.engagement_approval_workflow	<ul style="list-style-type: none"> <li>Type: string</li> <li>Default value: Engagement Approval</li> </ul>

## Roles installed with Audit Management

GRC: Audit Management adds the following roles.

Role title [name]	Description	Contains roles
Audit User [sn_audit.user]	Contains the reader role in sn_grc scopes, and the reader role in the Audit Management application. In addition to the inherited permissions, the audit user can be assigned audit tasks and create test templates and test plans. The audit user has read-only access to the Risk Management application and modules and the Policy and Compliance Management application and modules.	<ul style="list-style-type: none"> <li>sn_grc.reader</li> <li>sn_grc.user</li> </ul>
Audit Manager [sn_audit.manager]	Contains the reader, user, and manager roles in sn_grc scopes, and the reader and user roles in the Audit Management application. In addition to the inherited permissions, the audit manager can create authority documents, citations, policies, policy statements, and controls.	<ul style="list-style-type: none"> <li>sn_grc.reader</li> <li>sn_grc.user</li> <li>sn_grc.manager</li> <li>sn_audit.user</li> </ul>

Role title [name]	Description	Contains roles
Audit Admin [sn_audit.admin]	Contains the reader, user, manager, and admin roles in sn_grc scopes, and the reader, user, and manager roles in the Audit Management application. In addition to the inherited permissions, the audit admin can delete engagements, audit tasks, test templates, and test plans.	<ul style="list-style-type: none"> <li>sn_grc.reader</li> <li>sn_grc.user</li> <li>sn_grc.manager</li> <li>sn_grc.admin</li> <li>sn_audit.user</li> <li>sn_audit.manager</li> </ul>
Audit Developer [sn_audit.developer]	Contains the reader, user, manager, and admin roles in sn_grc scopes, and the reader, user, manager, and admin roles in the Audit Management application. In addition to the inherited permissions, the audit developer can add and delete audit report templates.	<ul style="list-style-type: none"> <li>sn_grc.reader</li> <li>sn_grc.user</li> <li>sn_grc.manager</li> <li>sn_grc.admin</li> <li>sn_audit.user</li> <li>sn_audit.manager</li> <li>sn_audit.admin</li> </ul>
External Auditor [sn_audit.external_auditor]		External auditors can be assigned as auditors for an engagement and can be assigned to audit tasks. They can view closed engagements, audit tasks that are assigned to them, and closed audit tasks. If the Policy and Compliance Management plugin or Risk Management plugins are installed, they can also view published policies and controls and risks in the Monitor state.

## Client scripts installed with Audit Management

GRC: Audit Management adds the following client scripts.

Client script	Table	Description
Design effectiveness update	Control Test [sn_audit_control_test]	Updates the control effectiveness when the design effectiveness changes.
Hide related list based on active plugin	Engagement [sn_audit_engagement]	If the Policy and Compliance Management or Risk Management plugins are not installed, hides certain Related Lists.
Hide workbench buttons	Engagement [sn_audit_engagement]	Hides extra header buttons plus the Edit and Validate buttons from the footer of the engagement form.

Client script	Table	Description
Operation effectiveness update	Control Test [sn_audit_control_test]	Updates the control effectiveness when the operation effectiveness changes.
Populate fields when Test Plan changes	Control Test [sn_audit_control_test]	Updates the expectations and assessment procedures whenever the test plan field is updated.
Populate fields from template	Test Plan [sn_audit_test_plan]	Certain fields on the test plan are populated from fields on the test template.
Populate planned end on duration change	Engagement [sn_audit_engagement]	Populates the planned end date if the planned start is populated and the duration changes.
Populate planned end on effort change	Audit Task [sn_audit_task]	Populates the planned end date when the planned duration changes.
Populate planned end on start change	Audit Task [sn_audit_task]	Populates the planned end when the planned start date changes.
Populate planned end on start changed	Engagement [sn_audit_engagement]	Populates the planned end date based on the planned start and planned duration.
Set Control Effectiveness	Control Test [sn_audit_control_test]	Sets the control effectiveness to none when a control test is closed as incomplete.
Show annotation message in engagement	Engagement [sn_audit_engagement]	Shows the annotation message in the workbench before validating the engagement.
Validate actual end date	Audit Task [sn_audit_task]	Validates that the actual end date is after the actual start date, and the actual end is on or before the engagement actual end.
Validate actual end date	Engagement [sn_audit_engagement]	Validates that the actual end date is after the actual start date.
Validate actual start date	Engagement [sn_audit_engagement]	Validates that the actual start date is before the actual end date.
Validate actual start date	Audit Task [sn_audit_task]	Validates that the actual start date is before the actual end date, and the actual start is after the actual start of the engagement.

Client script	Table	Description
Validate audit end date	Engagement [sn_audit_engagement]	Validates that the audit end date is after the audit start date.
Validate audit start date	Engagement [sn_audit_engagement]	If the engagement is populated, validates that the audit start date is before the audit end date.
Validate planned start date	Audit Task [sn_audit_task]	Validates that the planned start date is greater than or equal to the planned start date.
Workbench event listener	Engagement [sn_audit_engagement]	Refreshes the Profiles Related List for the workbench.

## Script includes installed with Audit Management

GRC: Audit Management adds the following script includes.

Script include	Description
AuditAjax	AJAX functions for Audit Engagement and Control Test forms.
AuditRollupUtils	Utilities for rolling up data from audit tasks to engagement.
AuditUtils	Utility functions in the Audit.
AuditWorkbenchAjaxService	Ajax utility responsible for fetching data required to draw the Audit Workbench.
AuditWorkbenchUtils	Utilities for the audit workbench and timeline.
GRCI18nUtils	Utilities for internationalizing GRC Workbench.

## Business rules installed with Audit Management

GRC: Audit Management adds the following business rules.

Business rule	Tables	Description
Add control to engagement	Control [sn_compliance_control]	Automatically relates a control to all engagements that are in the validate or fieldwork states and associate with the control profile
Add risk to engagement	Risk [sn_risk_risk]	Automatically relates a risk to all engagements that are in the validate or fieldwork states and associate with the risk profile



Business rule	Tables	Description
Add test plan to engagement	Test Plan [sn_audit_test_plan]	Automatically relates a test plan to all engagements that are in the validate or fieldwork states and associate with the test plan profile
Associate records when validated	Engagement [sn_audit_engagement]	Associates all risks, controls, and test plans associated with the profile when a profile is associated with an engagement in the Validate or Fieldwork states
Associate to engagement after scoped	Profile to Engagement [sn_audit_m2m_profile_engagement]	Associates all risks, controls, and test plans associated with an engagement scoped profiles when the engagement moves from the Scope state to the Validate state
Auto-approve if no approvers	Engagement [sn_audit_engagement]	If the Approvers field is empty, automatically moves an engagement from Awaiting Approval to Follow Up
Auto-close if no issues or tasks	Engagement [sn_audit_engagement]	If there are no open issues or tasks associated with the engagement, automatically moves an engagement from the Follow Up state to the Closed state
Check close incomplete	Control Test [sn_audit_control_test]	If a control test is Closed Incomplete, set the Control effectiveness field to none
Close Engagement	<ul style="list-style-type: none"> <li>Audit Task [sn_audit_task]</li> <li>Issue [sn_grc_issue]</li> </ul>	If there are no longer any open audit tasks or issues, automatically closes an engagement in Follow up
Control Effectiveness	Control Test [sn_audit_control_test]	Updates the control effectiveness based on changes to the design or operation effectiveness
Create issue if test ineffective, closed	Control Test [sn_audit_control_test]	If a control test is closed as ineffective, create an issue
Disassociate records upon deletion	Profile to Engagement [sn_audit_m2m_profile_engagement]	Disassociates risks, controls, and test plans when a relationship between a profile and engagement is removed

Business rule	Tables	Description
Populate fields when Test plan changes	Control Test [sn_audit_control_test]	Updates the expectations, assessment procedures, duration, and control whenever a control test of a test plan changes
Prevent duplicate association	Profile to Engagement [sn_audit_m2m_profile_engagement]	Prevents duplicate many-to-many relationships between profiles and engagements
Prevent picking retired control	<ul style="list-style-type: none"> <li>Control Test [sn_audit_control_test]</li> <li>Test Plan [sn_audit_test_plan]</li> </ul>	Prevents creating a control test or test plan against a retired control
Run approval workflow	Engagement [sn_audit_engagement]	Runs the approval workflow for engagements
Scratchpad to check active plugin	Engagement [sn_audit_engagement]	Sets scratchpad variables based on whether GRC: Risk Management, GRC: Policy and Compliance Management, and GRC: Profiles are installed
Set percent complete to 100 if no task	Engagement [sn_audit_engagement]	If the engagement is Closed Complete or Closed Incomplete with no tasks, set the percent complete of an engagement to 100
Set popup scratchpad	Engagement [sn_audit_engagement]	Sets scratchpad variables used to display dialogs
Set workbench display scratchpad	Engagement [sn_audit_engagement]	Set scratchpad variables used in the Engagement view
Start Control Test approval workflow	Control Test [sn_audit_control_test]	Runs the approval workflow for control tests
Update parent task percent complete	Audit Task [sn_audit_task]	Updates the parent task Percent complete when a child task is closed
Update planned end date	<ul style="list-style-type: none"> <li>Audit Task [sn_audit_task]</li> <li>Engagement [sn_audit_engagement]</li> </ul>	Updates the End date of an engagement or audit task whenever the Duration changes
Validate start and end dates	<ul style="list-style-type: none"> <li>Audit Task [sn_audit_task]</li> <li>Engagement [sn_audit_engagement]</li> </ul>	Validates that the planned start is before the planned end and that the actual start is before the actual end, and that the audit period start is before the audit period end

Business rule	Tables	Description
Validate task date with engagement date	Audit Task [sn_audit_task]	Validates that the planned start and planned end date of an audit task are within the time defined by the engagement planned start and planned end date. Similar validation is done for the actual work start and actual work end

## Engagement Overview

The Engagement Overview is contained in the Audit Management application and provides an executive view into audit results, engagement breakdowns by task, and allows areas of concern to be identified quickly.

The Engagement Overview module displays audit information that is tailored to the role of the user.

### Audit Engagement Overview

Users with the Audit Administrator and Audit Manager roles view the Audit Engagement Overview. It contains the following reports in the base system.

**Table 55: Audit Engagement Overview reports**

Name	Visual	Description
Engagement Results	Column Chart	Displays an overall count of audit engagements conducted for each profile. The chart is stacked to display the overall audit results for each profile.
Profiles by Engagement	Donut chart	Displays the total number of profiles included in the scope of each audit engagement.
Controls by Engagement	Donut chart	Displays the total number of controls included in scope of each audit engagement.
Profile	Drop down list	Select one or many profiles to view and compare their audit findings.
Select Engagement	Drop down list	Select one or many engagements to view and compare their audit findings.
Satisfactory Engagements	Single Score	Displays the number of engagements closed with a satisfactory result.

Name	Visual	Description
Adequate Engagements	Single Score	Displays the number of engagements closed with an adequate result.
Inadequate Engagements	Single Score	Displays the number of engagements closed with an inadequate result.
Control Test Results	Donut chart	The number of completed control tests, broken down by overall control effectiveness rating.
Issue Breakdown	Bar Chart	Count of issues grouped by engagement.
Audit Task Breakdown	Bar Chart	Count of audit tasks grouped by task type, stacked by state
Overdue Audit Tasks	List	List of open audit tasks that have exceeded the planned end date.

# Engagement Workbench

The Engagement Workbench provides a timeline view from which you can select an audit engagement to view details or create a new engagement.

**Figure 5: Audit Engagement**

The screenshot displays the 'Audit Engagement Workbench' interface. At the top right, there is a 'Create Engagement' button. Below the header, a red notification bar states '1 Engagement has exceeded its planned end date'. The main section is titled 'Audit Engagement Timeline' and includes date range selectors for '2016-05-23' and '2016-11-19'. A search filter is set to 'All of these conditions must be met' with the keyword 'are'. Below the filter, a timeline shows three engagement bars: 'Customer Support Review' (81%), 'Finance Department ...' (17%), and 'Finance Department Rev...' (0%). A central callout box titled 'Audit Engagement' prompts the user to 'Select an Audit Engagement from the Audit Engagement Timeline to view details or create a new Engagement' and includes a 'Create Engagement' button.

## Create an engagement from Audit Workbench

Audit managers create engagements directly from the Workbench to manage audit information and collect profiles, controls, and control tests that are relevant to the audit.

Role required: sn\_audit.admin or sn\_audit.manager

1. Navigate to Audit Engagements Workbench .
2. Click Create Engagement.
3. Fill in the fields on the form, as appropriate.

**Table 56: Engagement form**

Field	Description
Name	The name of the engagement.
Assigned to	The user assigned to the engagement.
Description	A general description of the engagement.
Objectives	The stated objectives of the engagement.
Planned start date	The intended date the activity should begin.
Planned duration	The expected duration of this activity. As with actual duration, the planned duration shows total activity time and takes the activity schedule into consideration.
Audit period start	Date that work on the engagement is expected to begin.
Audit period end	Date that work on the engagement is expected to begin.
Auditors	The auditors assigned to the engagement.
Approvers	The approvers assigned to the engagement.

4. Click Create.

## Engagements

The audit engagement process involves creating, planning, scoping, and conducting engagements as well as reporting on engagement findings.

### Engagement process

The base system audit engagement process includes steps for scoping, validating, conducting, and approving engagement results. It also contains steps for following up on open audit tasks and issues, and finally closing out the audit engagement.

Table 57: States of the engagement process

State	Description
Scope	<p>During the Scope state, audit managers define which profiles will be involved in the audit engagement. For example, for a financial audit, one may include all business services that the finance department relies on and the finance department itself.</p> <p>See <a href="#">Add profiles to an engagement scope</a> on page 131.</p>
Validate	<p>After an engagement has moved to the Validate state, all of the risks, controls, and test plans associated with the profiles in the engagement's scope will be associated with the audit. Indicator results that were collected during the engagement's audit period will also be associated with the audit. Audit managers can review the risks, controls, test plans, and indicator results, and update the engagement's scope, if necessary. Audit managers can also begin creating and planning audit tasks for the engagement.</p> <p>To move an engagement into the Validate state, click Validate on any engagement currently in the Scope state.</p>
Fieldwork	<p>Auditors complete their assigned audit tasks during the Fieldwork state. These tasks include control testing, interviews, walkthroughs, and other activities. Issues that are found during control testing are associated with the engagement. Auditors can also create general issues associated with the engagement. Audit managers can create additional audit tasks as needed. When the audit is done, audit managers specify the result of the engagement, whether it's satisfactory, adequate or inadequate, and provide details on their opinion.</p> <p>To move an engagement into the Fieldwork state, click Advance to Fieldwork on any engagement currently in the Validate state.</p> <p>See <a href="#">Audit tasks</a> on page 136.</p>

State	Description
Awaiting Approval	<p>During the "Awaiting Approval" state, the approvers specified in the engagement's Approvers field review the results of the audit tasks conducted and the issues that were created. After reviewing the results of the engagements, approvers approve or reject the engagement.</p> <p>To move an engagement into the Awaiting Approval state, click Request approval on any engagement currently in the Fieldwork state.</p> <p>See <a href="#">Approve or reject an engagement</a> on page 131.</p>
Follow Up	<p>After an engagement has been approved, if there are any remaining open tasks or issues associated with the engagement, the engagement automatically goes into the Follow Up state. During this stage, auditors must close out all remaining issues and tasks before the engagement will be marked as complete.</p>
Closed	<p>Engagements move into the "Closed" state under one of three conditions:</p> <ul style="list-style-type: none"> <li>• The engagement is closed as incomplete during the Scope, Validate, or Fieldwork states.</li> <li>• There are no open audit tasks or issues after the engagement is approved. In this case, the engagement automatically moves from the Awaiting Approval state to the Closed state.</li> <li>• All of the follow up issues and tasks are closed out. In this case, the engagement automatically moves from the Follow Up state to the Closed state.</li> </ul>

## Create an engagement

Audit managers create engagements to manage audit information and collect profiles, controls, and control tests that are relevant to the audit.

Role required: sn\_audit.admin or sn\_audit.manager

1. Navigate to Audit Engagements Create New .
2. Fill in the fields on the form, as appropriate.



Table 58: Engagement form

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
State	<ul style="list-style-type: none"> <li>• New</li> <li>• Analyze</li> <li>• Respond</li> <li>• Review</li> <li>• Closed</li> </ul>
Name	The name of the engagement.
Percent complete	Read-only field that is automatically populated with a number representing the percentage of the engagement that has been completed.
Assigned to	The user assigned to the engagement.
Auditors	The auditors assigned to the engagement.
Audit period start	Date that work on the engagement is expected to begin.
Approvers	The approvers assigned to the engagement.
Audit period end	Date that work on the engagement is expected to begin.
Description	A general description of the engagement.
Objectives	The stated objectives of the engagement.
Schedule	
Planned start date	The intended date the activity should begin.
Planned end date	The intended date the activity should end.
Planned duration	The expected duration of this activity. As with actual duration, the planned duration shows total activity time and takes the activity schedule into consideration.
Actual start date	The date that this activity actually began.
Actual end date	The date that this activity actually ended.
Actual duration	The actual duration of the project from project start to project closure. As with planned duration, the actual duration shows total project time and takes the project schedule into consideration.
Results	

Field	Description
Result	<ul style="list-style-type: none"> <li>Satisfactory</li> <li>Adequate</li> <li>Inadequate</li> </ul>
Opinion	Justification for the selected result.
Report	
Report template	The template to be used to generate the knowledge base article reporting the engagement results.
KB article	The most recently generated knowledge base article containing the engagement results
Activity Journal	
Additional comments	Customer-viewable comments.
Work notes	Comments that are viewable by the admin, audit manager.

3. Click Submit.

## Create an engagement from a previous engagement

Audit managers can create engagements from previous engagements to reduce the need to redefine the scope, auditors, and approvers for similar engagements that are conducted throughout the year.

Role required: sn\_audit.admin or sn\_audit.manager

1. Navigate to Audit Engagement All Engagements .
2. If necessary, clear the search filter criteria.
3. Open the engagement to copy from.
4. Right-click the header of the engagement and click Copy Engagement.

## Generate a KB article from an engagement

Audit managers can generate a KB article that summarizes the findings of an engagement so report findings can be communicated to executives.

Role required: sn\_audit\_manager

KB articles can be generated for engagements in the Awaiting approval, Follow up, and Closed complete states.

1. Navigate to Audit All Engagements .
2. Open the engagement record.
3. Fill in the fields on the Reports tab, as appropriate.

Table 59: Reports tab on engagement form

Field	Description
Report template	Select the report template to use for this KB article.
KB article	Read-only field that is automatically populated with a unique identification number.

4. Click Generate report.

## Approve or reject an engagement

Audit users that are assigned as approvers for an engagement can approve or reject engagements in the Awaiting Approval state.

Role required: sn\_audit.user

1. Navigate to Audit My Audit Approvals .
2. Open the approval record associate with the engagement.
3. Click Approve or Reject

One of the following actions occurs:

- If the engagement is approved and there are remaining open tasks or issues, it automatically moves into the Follow Up state.
- If the engagement is approved and there are no remaining open tasks or issues, it automatically moves into the Closed state.
- If the engagement is rejected, it automatically moves back to the Fieldwork state

## Add profiles to an engagement scope

Audit managers define which profiles will be involved in the audit engagement.

Role required: sn\_audit.manager or sn\_audit.admin

1. Navigate to Audit Engagements All Engagements .
2. Open an engagement in the Scope or Validate state.
3. In the Profiles related list, click Add.
4. Select the desired profiles that will be included in the audit engagement.
5. Click Add.

## GRC profile scoping

The Scoping module contains profiles and profile types for use in all GRC-related applications. They can be created for any record on any table.

The GRC: Profile plugin contains the Scoping module and is not visible to customers and requires activation of the Policy and Compliance Management plugin, the Risk Management plugin, or the Audit Management plugin.

Only one profile can exist for a record. That profile, however, can belong to many profile types. Profile types and profiles are used differently depending on the application:

- Risk managers use profile types and profiles to monitor risk exposure and perform risk assessments.
- Policy and compliance managers use profile types and profiles to create a system of internal controls and monitor compliance.

## Profiles

Profiles are the records that aggregate GRC information related to a specific item. Each profile is associated with a single record from any table in the application. Profiles cannot be created for items that do not have a record in a table in the platform.

## Profile Classes

Profile classes allow GRC managers to separate profiles for better distinction. For example, Business Service Profiles, Department Profiles, Business Unit Profiles, and the like.

## Profile Types

Profiles types are dynamic categories containing one or more profiles. Business logic automates the process of creating and categorizing any profiles in the system that meet the profile type conditions. Profile types are assigned to policy statements, which generate controls for every profile listed in the profile type.

## Create and edit a profile type

Administrators or managers in any of the GRC-related applications, create profiles types from which profiles are generated.

Role required: sn\_compliance.admin or sn\_compliance.manager, sn\_risk.admin or sn\_risk.manager, sn\_audit.admin or sn\_audit.manager

1. Navigate to one of the following locations:
  - Audit Scoping Profile Types .
  - Policy and Compliance Scoping Profile Types .
  - Risk Scoping Profile Types .

2. Do one of the following actions:

Option	Description
<b>To create a new profile type</b>	Click New.
<b>To edit a profile type</b>	Open the profile type.

3. Fill in the fields on the form, as appropriate.

**Table 60: Profile type**

Name	Description
Name*	The name of the profile type.

Name	Description
Description	An explanation of the profile type with any additional information about the profile type that a user will find helpful.
Table*	The table from which the profile type conditions identify the records to create profiles.
Condition	Filter conditions to restrict which profiles belong to a specific profile type.
Use owner field	Select the check box to indicate that a default owner field should be used when generating new profiles.
Default owner	The field on the table specifying the person who owns any new profiles generated from the profile type.
Default profile class	<p>Set the default profile class.</p> <p>Generated profiles copy this default profile class under the following conditions:</p> <ul style="list-style-type: none"> <li>when the profile's class is empty and it's associated to a profile type that has a default profile class</li> <li>when a profile is created under a profile type that has a default profile class</li> </ul> <p>The existing profile's class is updated under the following conditions:</p> <ul style="list-style-type: none"> <li>The profile type's table changes</li> <li>The profile type's condition changes</li> <li>The profile type's active field is ik;8,'</li> <li>The profile type's default profile class changes</li> </ul>

**Note:** \* indicates a mandatory field.

4. Click Submit.

## Generate a profile from a profile type

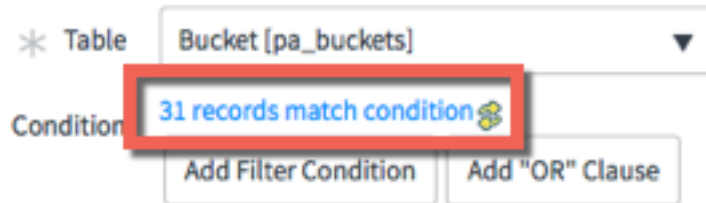
Profiles are generated automatically from profile types in any of the GRC-related applications.

Role required: sn\_compliance.admin or sn\_compliance.manager, sn\_risk.admin or sn\_risk.manager, sn\_audit.admin or sn\_audit.manager

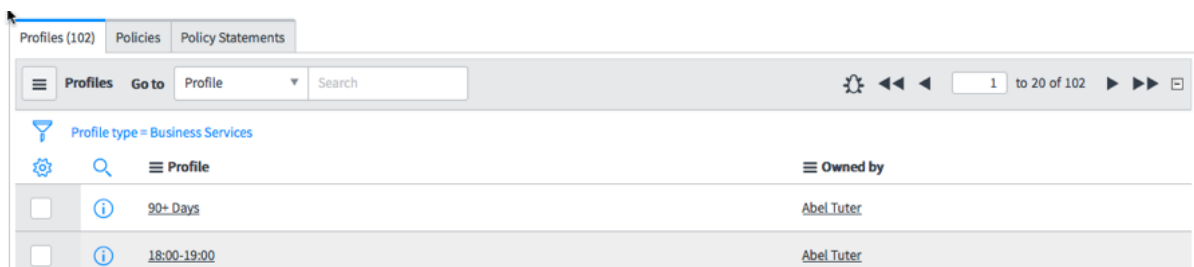
- Navigate to one of the following locations:
  - Audit Scoping Profile Types
  - Policy and Compliance Scoping Profile Types
  - Risk Scoping Profile Types

2. Open the Profile Type record.
3. Add or modify any conditions, as necessary.

Changing the Table, changes the number of records matching the condition.



4. Assign the Owner field.
  5. Click Update.
- A profile is generated for every record that matches the filter condition.



## Deactivate a profile

When a profile is deactivated, all the controls related to that profile are retired, and the indicators and test plans associated to those controls are marked in-active.

Role required: grc\_manager

The owner of the profile can edit the profile record and deactivate it.

1. Navigate to one of the following locations:
  - Audit Scoping All Profiles
  - Policy and Compliance Scoping All Profiles
  - Risk Scoping All Profiles
2. Open the profile record.
  - If the Active check box is selected, then the profile is active.
  - If the Active check box is not selected, then the profile is inactive.
3. Click Update.
  - All associated controls change to the retired state.

- All the indicators and test plans associated with the retired control are marked in-active.

## Reactivate a profile

When a profile is reactivated, associated controls and risks return to the draft state and the indicators and test plans return to active.

Role required: grc\_manager

The owner of the profile can edit the profile record and reactivate it.

1. Navigate to one of the following locations:
  - Audit Scoping All Profiles
  - Policy and Compliance Scoping All Profiles
  - Risk Scoping All Profiles
2. Open the profile record.
3. In the profile, select the check box marked Active.
4. Click Update.

All associated controls, risks, indicators, and test plans are also re-activated or retired.

## Create a profile class

GRC managers create profile classes representing the types of things that will be part of the dependency model. Reports can be filtered to define relationships between the different profile classes. A profile class defines what a profile actually is. It differs from a profile type (for example, Business Services and Critical Business Services), in that a profile can belong to many profile types but a profile can have only one profile class (for example, Business Service).

Role required: sn\_grc.manager

1. Navigate to one of the following locations:
  - Audit Scoping Profile Classes
  - Policy and Compliance Scoping Profile Classes
  - Risk Scoping Profile Classes
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 61: Authority Document**

Field	Value
Name	Name of the profile class.
Roll up to	Select dependencies to other profiles. Useful for reporting how your lower-level operational risks impact corporate-level risks.

Field	Value
Is Root	<p>Select the check box to indicate that this is the highest level class.</p> <hr/> <p><b>Note:</b> Only one root class is allowed and it cannot roll up to another class.</p> <hr/>

4. Click Submit.

## Assign profiles to classes

GRC managers assign profiles to classes for the filtering of reports and to define relationships between the different classes of business services.

Role required: sn\_compliance.manager

1. Navigate to one of the following locations:
  - Audit Scoping All Profiles
  - Policy and Compliance Scoping All Profiles
  - Risk Scoping All Profiles
2. Open the profile record.
3. Assign the Class.
4. Click Update.

## Add profiles to an engagement scope

Audit managers define which profiles will be involved in the audit engagement.

Role required: sn\_audit.manager or sn\_audit.admin

1. Navigate to Audit Engagements All Engagements .
2. Open an engagement in the Scope or Validate state.
3. In the Profiles related list, click Add.
4. Select the desired profiles that will be included in the audit engagement.
5. Click Add.

## Audit tasks

Audit tasks are completed throughout an engagement and provide documented evidence that the organization is complying with external regulations and internal policies.

When audit tasks are created or reassigned, a notification is sent to the assigned user. A notification is also sent when the task reaches 75% of its planned duration.

## Create an activity

After defining a control, audit managers create activities that explore and provide documented evidence of whether the associated control is operating correctly.



Role required: sn\_audit.admin and sn\_audit.manager

1. Navigate to Audit Engagements All Engagements .
2. Open the engagement for the audit task you want to create.  
Assign audit tasks to engagement in one of the following states:
  - Validate
  - Fieldwork
  - Awaiting approval
3. In the Audit Tasks Related List, click New.
4. In the Audit Tasks Interceptor, click Activity.
5. Fill in the fields on the form, as appropriate.

**Table 62: Activity form**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
State	<ul style="list-style-type: none"> <li>• Open</li> <li>• Work in Progress</li> <li>• Review</li> <li>• Closed Complete</li> <li>• Closed Incomplete</li> <li>• Closed Skipped</li> </ul>
Parent	The parent audit task.
Assigned to	The user assigned to this activity.
Short description	A brief and general description of the activity.
Description	A more detailed explanation of the activity.
Schedule	
Planned start date	The intended date the activity should begin.
Planned end date	The intended date the activity should end.
Planned duration	The expected duration of this activity. As with actual duration, the planned duration shows total activity time and takes the activity schedule into consideration.
Actual start date	The date that this activity actually began.
Actual end date	The date that this activity actually ended.
Actual duration	The actual duration of the project from project start to project closure. As with planned duration, the actual duration shows total project time and takes the project schedule into consideration.
Activity	

Field	Description
Additional comments	Customer-viewable comments.
Work notes	Comments that are viewable by the audit manager and audit manager.

6. Click Submit.

## Create a control test from an engagement

After defining a control, audit managers create control tests that run periodically and provide documented evidence of whether the associated control is operating correctly.

Role required: sn\_audit.admin and sn\_audit.manager

1. Navigate to Audit Engagements All Engagements .
2. Open the engagement for the audit task you want to create.  
Assign audit tasks to engagement in one of the following states:
  - Validate
  - Fieldwork
  - Awaiting approval
3. In the Audit Tasks Related List, click New.
4. In the Audit Tasks Interceptor, click Control Test.
5. Fill in the fields on the form, as appropriate.

**Table 63: Control test form**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
State	<ul style="list-style-type: none"> <li>• Open</li> <li>• Work in Progress</li> <li>• Review</li> <li>• Closed Complete</li> <li>• Closed Incomplete</li> <li>• Closed Skipped</li> </ul>
Parent	The parent audit task.
Control effectiveness	The effectiveness of the control.
Assigned to	The user assigned to this control test.
Issue	The issue related to this control test.
Test plan	The test plan associated with this control test.
Short description	A brief and general description of the control test.

Field	Description
Schedule	
Planned start date	The intended date the control test should begin.
Planned end date	The intended date the control test should end.
Planned duration	The expected duration of this control test. As with actual duration, the planned duration shows total activity time and takes the control test schedule into consideration.
Actual start date	The date that this control test actually began.
Actual end date	The date that this control test actually ended.
Actual duration	The actual duration of the control test from control test start to control test closure. As with planned duration, the actual duration shows total project time and takes the control test schedule into consideration.
Design Test	
Design effectiveness	<ul style="list-style-type: none"> <li>• Effective</li> <li>• Ineffective</li> </ul>
Design expectations	
Design assessment procedures	
Design results	
Operation Test	
Operation effectiveness	<ul style="list-style-type: none"> <li>• Effective</li> <li>• Ineffective</li> </ul>
Operation expectations	
Operation assessment procedures	
Operation results	
Activity Journal	
Work notes	Comments that are viewable by the audit manager and audit manager.
Additional comments	Customer-viewable comments.

6. Click Submit.

## Create an interview

After defining a control, audit managers create interviews with control owners to discuss and provide documented evidence of whether the associated control is operating correctly.

Role required: sn\_audit.admin and sn\_audit.manager

1. Navigate to Audit Engagements All Engagements .
2. Open the engagement for the audit task you want to create.  
Assign audit tasks to engagement in one of the following states:
  - Validate
  - Fieldwork
  - Awaiting approval
3. In the Audit Tasks Related List, click New.
4. In the Audit Tasks Interceptor, click Interview.
5. Fill in the fields on the form, as appropriate.

**Table 64: Interview form**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
State	<ul style="list-style-type: none"> <li>• Open</li> <li>• Work in Progress</li> <li>• Review</li> <li>• Closed Complete</li> <li>• Closed Incomplete</li> <li>• Closed Skipped</li> </ul>
Parent	The parent audit task.
Assigned to	The user assigned to this interview.
Short description	A brief and general description of the interview.
Description	A more detailed explanation of the interview.
Schedule	
Planned start date	The intended date the interview should begin.
Planned end date	The intended date the interview should end.
Planned duration	The expected duration of this interview. As with actual duration, the planned duration shows total activity time and takes the interview schedule into consideration.
Actual start date	The date that this interview actually began.
Actual end date	The date that this interview actually ended.

Field	Description
Actual duration	The actual duration of the interview from interview start to interview end. As with planned duration, the actual duration shows total project time and takes the interview schedule into consideration.
Assignment	
Primary Contact	The user to contact for this interview.
Other Contacts	Other users to contact for this interview, if the primary contact is unavailable.
Notes	Additional notes about the interview contacts.
Activity	
Additional comments	Customer-viewable comments.
Work notes	Comments that are viewable by the audit administrator and audit manager.

## Create a walkthrough

After defining a control, audit managers create walk throughs that will be conducted to observe and provide documented evidence of whether the associated control is operating correctly.

Role required: sn\_audit.admin and sn\_audit.manager

1. Navigate to Audit Engagements All Engagements .
2. Open the engagement for the audit task you want to create.  
Assign audit tasks to engagement in one of the following states:
  - Validate
  - Fieldwork
  - Awaiting approval
3. In the Audit Tasks Related List, click New.
4. In the Audit Tasks Interceptor, click Walkthrough.
5. Fill in the fields on the form, as appropriate.

**Table 65: Walkthrough form**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.

Field	Description
State	<ul style="list-style-type: none"> <li>• Open</li> <li>• Work in Progress</li> <li>• Review</li> <li>• Closed Complete</li> <li>• Closed Incomplete</li> <li>• Closed Skipped</li> </ul>
Parent	The parent audit task.
Assigned to	The user assigned to this walkthrough.
Short description	A brief and general description of the walkthrough.
Description	A more detailed explanation of the walkthrough.
Schedule	
Planned start date	The intended date the walkthrough should begin.
Planned end date	The intended date the walkthrough should end.
Planned duration	The expected duration of this walkthrough. As with actual duration, the planned duration shows total activity time and takes the walkthrough schedule into consideration.
Actual start date	The date that this walkthrough actually began.
Actual end date	The date that this walkthrough actually ended.
Actual duration	The actual duration of the walkthrough from walkthrough start to walkthrough end. As with planned duration, the actual duration shows total project time and takes the walkthrough schedule into consideration.
Walkthrough	
Primary Contact	The user to contact for this walkthrough.
Other Contacts	Other users to contact for this walkthrough, if the primary contact is unavailable.
Execution Steps	Detail the activities to be performed during the walkthrough.
Explanation	Intended purpose of the walkthrough.
Additional Information	Additional information the user conducting the walkthrough needs to be aware of.
Results	Details of what transpired during the walkthrough.

Field	Description
Activity	
Additional comments	Customer-viewable comments.
Work notes	Comments that are viewable by the audit manager and audit manager.

6. Click Submit.

## Audit testing

An audit engagement may include control testing activities during which controls are evaluated for design and operational effectiveness.

### Test Templates and Test Plans

To conduct control testing, before an engagement starts, audit managers create test plans for the relevant controls. Audit managers can use test templates to create multiple test plans for similar controls at one time.

During the Validate state of an audit engagement, the test plans that are associated with the controls in the engagement's scope are automatically associated with the engagement. Audit managers can generate control tests from those associated test plans and create individual control tests as needed.

### Create a test template

Test templates allow audit managers to quickly create many test plans using much of the same testing criteria.

Role required: sn\_audit.admin, sn\_audit.manager, or sn\_audit.user

1. Navigate to Audit Audit Testing Test Templates .
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 66: Test template form**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
Duration	Duration of the test.
Short description	A brief and general description of the test template.
Design Test*	
Design expectations	Expectations of how a control is designed.
Design assessment procedures	Document how to assess if a control is designed effectively.

Field	Description
Operation Test*	
Operation expectations	Expectations of how a control operates.
Operation assessment procedures	Document how to assess if a control is operating effectively

4. Click Submit.

## Relate a test template to a policy statement

Audit owners can create generic control test templates for a policy statement, avoiding the creation of individual control test plans for every control.

Role required: sn\_audit.admin or sn\_audit.manager

1. Navigate to Audit Audit Testing Test Templates .
2. Open the test template record.
3. Select a policy statement and click Update.

## Create a test plan

Test plans can be created from scratch or based on test templates and describe how a feature is to be tested.

Role required: admin

1. Navigate to Audit Audit Testing Test Plans .
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 67: Test template form**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
Control	The control that this test plan covers.  <b>Note:</b> This field is only visible when the Policy and Compliance Management plugin is activated.
Duration	The expected duration of the test.
Test Template	The related test template.
Short description	A brief and general description of the test plan.
Design Test*	
Design expectations	Expectations of how a control is designed.



Field	Description
Design assessment procedures	Document how to assess if a control is designed effectively.
Operation Test*	
Operation expectations	Expectations of how a control operates.
Operation assessment procedures	Document how to assess if a control is operating effectively.

4. Click Submit.

## Create multiple test plans from a test template

If GRC: Policy and Compliance Management is installed, a test template can be used to create test plans for all of the controls associated with the test plan's policy statement.

Role required: sn\_audit.manager or sn\_audit.admin

1. Navigate to Audit Audit Testing Test Templates .
2. Select the test template from which to generate test plans.
3. Click the Create Test Plans for All Controls related link.

---

**Note:** This link is only visible if there are controls associated with the test plan's policy statement that have not yet had a test plan generated from the current test template.

---

## GRC continuous monitoring

Continuous monitoring involves activities related to identifying and creating key risk and controls indicators. Supporting information can be collected for those indicators through automatic data collection or manual tasks. Indicator results are then used to create issues for controls, update risk scores, and provide supporting information for audit activities and control testing.

### Indicators

Indicators collect data to monitor controls and risks, and collect audit evidence. Indicators monitor a single control or risk.

### Indicator templates

Indicator templates allow the creation of multiple indicators for similar controls or risks.

## Create a GRC indicator

Indicator data for controls, risk, and audit evidence are measured differently depending on the GRC-related application.

Role required: compliance\_admin or compliance\_manager, risk\_admin or risk\_manager, audit\_admin or audit\_manager

1. Navigate to one of the following locations:

- Policy and Compliance Indicators Indicators .
  - Risk Indicators Indicators .
  - Audit Indicators Indicators .
2. Select New.
  3. Fill in the fields on the form, as appropriate.

Table 68: Indicator

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
Active	Check box that determines whether the indicator is active.
Name	Name of the indicator.
Item	The related control or risk.
Template	The related indicator template.
Applies to	The profile related to the Item.
Owner	The indicator owner.
Owning group	The group that owns the indicator.
Override Template	Click to override the indicator template associated to this indicator
Last result passed	Read-only field indicating whether last result passed.
Schedule	
Collection frequency	Select the collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule.
Next run time	Read-only field that is automatically populated with the next collection time for indicator results.
Method	
Type	Results can be gathered manually using task assignment or automatically using basic filter conditions, Performance Analytics, or a script. <ul style="list-style-type: none"> <li>• Manual</li> <li>• Basic</li> <li>• Script</li> </ul>
Short Description	If Type is Manual, this field is present. Brief description of the issue.

Field	Description
Instructions	If Type is Manual, this field is present. Instructions for the collection of indicator results.
Value Mandatory	If Type is Manual, this field is present.
Passed/Failed	If Type is Basic, this field is present. Indicator passes or fails.
PA Threshold	If Type is PA Indicator, this field is present. The associated PA Threshold.
Script	If Type is Script, this field is present. Script that obtains the desired system information.
Supporting Data	
Table	Use supporting data to gather supporting evidence from other applications.
Supporting data fields	Supporting data fields based on the selected table.

4. Click Submit.

## Create a GRC indicator template

Compliance or risk managers create indicator templates from which many indicators can be created.

Role required: compliance\_admin or compliance\_manager, risk\_admin or risk\_manager, audit\_admin or audit\_manager

1. Navigate to one of the following locations:
  - Policy and Compliance Indicators Indicator Templates .
  - Risk Indicators Indicator Templates .
  - Audit Indicators Indicator Templates .
2. Select New.
3. Fill in the fields on the form, as appropriate.

**Table 69: Indicator template**

Field	Description
Name	Name of the indicator.
Active	Check box that determines whether the indicator template is active.
Content	The related policy or risk statement.
Schedule	
Collection frequency	Select the collection frequency for indicator results. Indicator tasks and results are generated automatically based on the indicator schedule.

Field	Description
Next run time	Read-only field that is automatically populated with the next collection time for indicator results.
Method	
Type	Results can be gathered manually using task assignment or automatically using basic filter conditions, Performance Analytics, or a script. <ul style="list-style-type: none"> <li>• Manual</li> <li>• Basic</li> <li>• PA Indicator</li> <li>• Script</li> </ul>
Short Description	If Type is Manual, this field is present. Brief description of the issue.
Instructions	If Type is Manual, this field is present. Instructions for the collection of indicator results.
Value Mandatory	If Type is Manual, this field is present.
Passed/Failed	If Type is Basic, this field is present. Indicator passes or fails.
PA Threshold	If Type is PA Indicator, this field is present. The associated PA Threshold.
Script	If Type is Script, this field is present. Script that obtains the desired system information.
Supporting Data	
Collect Supporting Data	Check to gather supporting evidence from other applications.

4. Click Submit.

## GRC issues management

Issues can be created manually to document audit observations, remediations, or to accept any problems. They are automatically generated from indicator results, attestation results, or control test effectiveness.

An issue is created automatically when:

- Issue - An indicator fails
- Control issue - A control attestation is completed indicating that the control is Not implemented
- Control test issue - A control test is closed complete with the control effectiveness set to Ineffective
- Other issue - is created by the user manually

Remediating an issue marks an intention to fix the underlying issue causing the control failure or risk exposure. Accepting an issue marks an intention to create an exception for a known control failure or risk.

Controls that are Accepted remain in a non-compliant state until the control is reassessed. In this way, the issue can be used to document observations during audits.

## Create a GRC issue manually

Manually create issues to document audit observations, the intention of remediations, or to accept any problems.

Role required: (per product)

- In GRC: `compliance_admin`, `compliance_manager`, or `sn_compliance.user`
- In Risk Management: `_admin`, `risk_manager`, or `sn_risk.user`
- In Audit Management: `audit_admin`, `audit_manager`, or `audit_admin` or `sn_audit.user`

1. Navigate to one of the following locations:
  - Audit Issues Create New .
  - Policy and Compliance Issues Create New .
  - Risk Issues Create New .
2. Fill in the fields on the form, as appropriate.

**Table 70: Issue**

Field	Description
Number	Read-only field that is automatically populated with a unique identification number.
State	<ul style="list-style-type: none"> <li>• New</li> <li>• Analyze</li> <li>• Respond</li> <li>• Review</li> <li>• Closed</li> </ul>
Assignment group	A group assigned to the issue.
Assigned to	The user assigned to the issue.
Priority	Priority for this issue: <ul style="list-style-type: none"> <li>• 1 - Critical</li> <li>• 2 - High</li> <li>• 3 - Moderate</li> <li>• 4 - Low</li> <li>• 5 - Planning</li> </ul>
Short description	Brief description of the issue.
Details	
Profile	The related profile.
Item	The related control or risk.
Description	A more detailed explanation of the issue.

Field	Description
Recommendation	The recommended action to resolve this issue.
Dates	
Planned start date	Date and time that work on the issue is expected to begin.
Planned end date	Date and time that work on the issue is expected to end.
Planned duration	Estimated amount of work time. Calculated using the Planned start date and Planned end date.
Actual start date	Time when work began on this issue
Actual end date	Time when work on this issue was completed.
Actual duration	Amount of work time. Calculated using the Actual start date and Actual end date.
Activity	
Work notes	Information about how to resolve the issue, or steps already taken to resolve it, if applicable. Work notes are visible to users who are assigned to the issue.
Additional comments (Customer visible)	Public information about the enhancement request.
Engagement	
Engagement	The related engagement.

3. Click Submit.

## Audit Management Administration

The Audit Management application provides properties associated with the audit report templates

See [Create an audit report template](#) on page 150

### Create an audit report template

Audit developers manage the audit report templates.

Role required: sn\_audit.developer

1. Navigate to Audit Administration Audit Report Templates .
2. Click New.
3. Fill in the fields on the form, as appropriate.

Table 71: Authority Document

Field	Value
Name	Name of the audit report template.
Type	<ul style="list-style-type: none"> <li>• Script</li> <li>• HTML</li> <li>• XML</li> </ul>
Is default	Check box to indicate that this template is used as the default template for all KB articles.
Script	The script code. This field is dependent on the Type field.
HTML	The HTML code. This field is dependent on the Type field.
XML	The XML code. This field is dependent on the Type field.

4. Click Submit.

## Governance, Risk, and Compliance (GRC) - Legacy

The ServiceNow® Governance, Risk, and Compliance (GRC) application enables you to document authority documents, policies, and risks and then design controls to enforce those documents and mitigate risk. Your organization can schedule and run control tests and/or conduct audits to gather compliance evidence and identify failures that require remediation.

### Explore

- [Video: Getting Started with GRC](#)
- [What is GRC? - Legacy](#) on page 170

### Planning

- [Whitepaper: 8 Simple Steps for Automating Governance, Risk, and Compliance \(GRC\)](#)

### Set up

- 
- 

### Administer

- 
- [Available GRC reports - Legacy](#) on page 188
- [GRC functional and technical roles - Legacy](#) on page 170

### Develop

- [Components installed with Governance, Risk, and Compliance \(GRC\) - Legacy](#) on page 153
- 
- [Developer training](#)
- [Developer documentation](#)

### Integrate

- [UCF authority document import process - Legacy](#) on page 235
- [UCF import properties - Legacy](#) on page 171

### Use

### Troubleshooting and get help

- [Ask or answer questions in the GRC community](#)

- [GRC authority documents and GRC citations - Legacy](#) on page 204
- [GRC risks, risk criteria, and risk approach rules - Legacy](#) on page 199
- [GRC audits, audit observations and remediation tasks - Legacy](#) on page 227
- [Search the HI knowledge base for known error articles](#)
- [Contact ServiceNow Support](#)

## Legacy migration

Customers currently using Legacy GRC [com.snc.governance] or Legacy Risk [com.sn\_risk] are not required to activate and migrate to the new functionality, but recommended.

### Migrate from Legacy GRC

A migration tool is provided to migrate Legacy GRC authority documents, policies, controls, risks, risk/task relationships, and/or control/risk relationships to the new GRC applications.

Role required: sn\_compliance.admin or sn\_risk.admin

---

**Note:** Customers currently using Legacy GRC [com.snc.governance] are not required to activate the plugin and migrate to the new functionality.

---

1. Navigate to Policy and Compliance Administration Migration .
2. Select the items to migrate.
3. Click Migrate.  
A summary of successfully migrated items is shown.

### Supported migration

After migrating from the Legacy GRC application, certain relationships between elements are maintained. Relationships for the following elements are maintained.

**Table 72: Supported GRC migration elements**

Legacy GRC	Migrated GRC
Authority Documents [grc_authoritative_source]	Authority Documents [sn_compliance_authority_document]
Citations [grc_authoritative_src_content]	Citations [sn_compliance_citation]
Policies [grc_policy]	Policies [sn_compliance_policy]
Controls [grc_control]	<ul style="list-style-type: none"> <li>• Controls [sn_compliance_control]</li> <li>• Policy Statement [sn_compliance_policy_statement]</li> </ul>
Risk Definitions [sn_risk_definition]	Risk Statements [sn_risk_definition]



Legacy GRC	Migrated GRC
Risks [grc_risk]	Risks [sn_risk_risk]
Control Test Definitions [grc_control_test_definition] - manual type	Indicator Template [sn_grc_indicator_template] - manual type
Risk Criteria Thresholds [grc_risk_criteria_threshold]	Risk Criteria [sn_risk_criteria]

## Unsupported migration

After migrating from the Legacy GRC application, not all functionality is automatically migrated.

Migration of the following elements or other custom functionality, while it is not supported, can be accomplished.

- Control Test Definitions [grc\_control\_test\_definition] - auto type and attestation type
- Audit Instances [grc\_audit]
- Audit Definitions [grc\_audit\_definitions]
- Control Tests [grc\_control\_test]
- Conditions [grc\_condition]
- Requirements [grc\_audit\_requirements]
- Activities [grc\_activity]
- Control Test Sample Data [grc\_control\_test\_sample\_data]
- Scope [grc\_entity]
- Observations [grc\_observations]
- Remediations [grc\_remediation]

## Components installed with Governance, Risk, and Compliance (GRC) - Legacy

Several types of components are installed with the Governance, Risk, and Compliance (GRC) plugin.

Demo data is available with governance, risk, and compliance. The demo data provides information including authority documents, controls, and control test definitions.

## Tables installed with Governance, Risk, and Compliance (GRC) - Legacy

Governance, Risk, and Compliance (GRC) installs the following tables.

Name	Description
Citation Relationship types [auth_content_rel_type]	Stores the definitions for the available relationships between different parts of an authority document.
Authority Document [grc_authoritative_source]	
Citation [grc_authoritative_src_content]	Stores the citations that are the individual components of authority documents.
Activity [grc_activity]	Stores the task-based activities used in GRC audits. Extends table: Task [task]
Audit [grc_audit]	Stores all audit instances. Extends table: Planned Task [planned_task]

Name	Description
Audit Definition [grc_audit_definition]	Stores all audit definitions.
Requirements [grc_audit_requirement]	Stores the relationship between an audit and a requirement. Extends table: Task [task]
Condition [grc_condition]	Stores the conditions used by advanced control tests.
Condition Collection [grc_condition_collection]	Stores condition collection for advanced control tests.
Control [grc_control]	Stores the definitions of how a policy is enforced.
Control Test [grc_control_test]	Stores the instances of a control being used in practice. Extends table: Planned Task [planned_task]
Control Test Definition [grc_control_test_definition]	Stores the definitions of how controls are verified. Extends table: Scheduled Script Execution [sysauto_script]
Control Test Sample Data [grc_control_test_sample_data]	Stores the sample data generated by control tests. Extends table: Task [task]
Observation [grc_observation]	Stores tasks which record information uncovered during the audit process.
Observation Affected Items [grc_observation_affected_item]	Stores affected items related to observations.
GRC UCF Authority Document [grc_ucf_authority_document]	Stores the latest authority documents downloaded from the UCF site. The data in this staging table is overwritten each time UCF authority documents are downloaded.
GRC UCF Citation [grc_ucf_citation]	Stores the latest citation downloaded from the UCF site. The data in this staging table is overwritten each time UCF authority documents are downloaded.
GRC UCF Control [grc_ucf_control]	Stores the latest controls downloaded from the UCF site. The data in this staging table is overwritten each time UCF authority documents are downloaded.
GRC UCF Difference [grc_ucf_difference]	Stores the differences between the existing GRC entities and the available UCF updates. The data in this table is rebuilt each time UCF authority documents are downloaded or updated in GRC.
GRC UCF Download Status [grc_ucf_download_status]	Stores the results of the latest UCF download, such as the file version downloaded and the duration. The data in this table is overwritten each time UCF authority documents are downloaded.

Name	Description
GRC UCF Control [grc_ucf_filter]	Stores all the information GRC uses to manage document counts in the document filter. These are the values displayed for each group in the filter screen. The data in this table is rebuilt each time UCF authority documents are downloaded or updated in GRC.
GRC Update Status [grc_ucf_update_status]	Stores all the information used to manage the update of UCF Authority Documents into GRC. These values are used to keep track of approval states of requested updates.
Audit Control Test Instances [m2m_audit_control_test]	Stores the relationship between an audit and a control test instance.
Audit Control Test Definition [m2m_audit_control_test_def]	Stores the relationship between an audit and a control test definition.
Audit Definition Control Test Definition [m2m_audit_def_control_test_def]	Stores the relationship between an audit definition and a control test definition.
Audit Definition Requirement [m2m_audit_def_requirement]	Stores the relationship between an audit definition and a requirement and a control test definition.
Audit Definition Entity [m2m_audit_definition_entity]	Stores the relationship between an audit definition and an entity (scope).
Audit Entity [m2m_audit_entity]	Stores the relationship between an audit and an entity (scope).
Citation Mapping [m2m_auth_src_con_auth_src_con]	Stores the mapping between two citation entries and their relationship.
Condition Collection Condition [m2m_condition_coll_condition]	Stores the relationship between a condition collection and a condition.
Control Citation [m2m_control_auth_src_content]	Stores the relationship between a citation and a control.
Control Authority Document [m2m_control_authoritative_source]	Stores the relationship between an authority document and a control.
Policy Control [m2m_control_policy]	Stores the relationship between a control and a policy.
Policy Citation [m2m_policy_auth_src_content]	Stores the relationship between a citation and a policy.
Policy Authority Document [m2m_policy_authoritative_source]	Stores the relationship between an authority document and a policy.
Policy Authority Document [m2m_risk_authoritative_source]	
Risk Control [m2m_risk_control]	Stores the relationship between a control and a risk.

## User roles installed with Governance, Risk, and Compliance (GRC) - Legacy

Governance, Risk, and Compliance (GRC) installs the following roles.

**Note:** Users with the ITIL role have access to the application and can edit control tests, remediation tasks, and audits.

Role	Description	Contains Roles
GRC Control Test Processor	Responsible for ensuring that a control test is executed, run, and managed properly.	<ul style="list-style-type: none"> <li>grc_compliance_reader</li> <li>grc_control_test_owner</li> </ul>
GRC Executive Approver	Responsible for approving any changes to authority documents, citations, and controls imported from UCF Authority Documents. Users with this role have access to their list of UCF document requests in the My Approvals module.	<ul style="list-style-type: none"> <li>grc_compliance_approver</li> <li>approver_user</li> </ul>
GRC External Auditor	Responsible for reviewing the control tests and the observations generated from them. These users have read-only access to all records involved in an audit and are external to the organization.	grc_audit_reviewer
GRC Internal Auditor	<p>Responsible for reviewing and auditing control test results, and managing observations for those results. These users have the following access:</p> <ul style="list-style-type: none"> <li>Read-only access to authority documents, citations, controls, risks, and policies.</li> <li>Read-only access to audit tables.</li> <li>Read-only access to control test instances assigned to an audit.</li> <li>Read-only access to observation instances assigned to them. This user can add a work note.</li> <li>Able to create observations.</li> </ul>	<ul style="list-style-type: none"> <li>grc_compliance_reader</li> <li>grc_audit_owner</li> </ul>

Role	Description	Contains Roles
grc_audit_definition_admin	Can create and edit Audit Definitions. Can read audit records and records associated with an audit.	<ul style="list-style-type: none"> <li>task_editor</li> <li>grc_audit_reader</li> <li>grc_control_test_reader</li> <li>grc_compliance_reader</li> </ul>
grc_audit_owner	Allows read-only access to audits, observations, remediations, and control tests for an audit assigned that user. Also allows writing and creation of observations, and work notes.	<ul style="list-style-type: none"> <li>grc_control_test_reader</li> <li>grc_audit_reader</li> </ul>
grc_audit_reader	Allows read-only access to audits, observations, remediations, and related tables.	
grc_audit_reviewer	Provides read-only access to audit and associated control test instances assigned to that user.	
grc_compliance_approver	Allows approval for any changes to authority documents, citations, controls, policies, and risks. Used for the approval workflow for changed/ updated entities.	<ul style="list-style-type: none"> <li>grc_compliance_reader</li> <li>grc_audit_reader</li> </ul>
grc_control_test_owner	Responsible for ensuring that controls are executed, run, and managed properly. These users can review control test definitions and control test instances and create observations. These users have the following access: <ul style="list-style-type: none"> <li>Read-only access to authority documents, citations, controls, risks, and policies.</li> <li>Read, write, update, and deactivate control test definitions. These users cannot change control test instances for automated tests.</li> <li>Read, write, and update control test instances for controls they own.</li> </ul>	grc_control_test_reader

Role	Description	Contains Roles
grc_control_test_reader	Can view control tests and control test definitions.	
grc_reports_user	Can view GRC report gauges.	

Script includes installed with Governance, Risk, and Compliance (GRC) - Legacy

Governance, Risk, and Compliance (GRC) adds the following script includes.

**Table 73: Script Includes**

Name	Description
AuthSourceProcessor	Generates a hierarchy of citations and relationships in the Policy [grc_policy] and Control [grc_control] tables.
ControlTestCreate	Creates records in the Control Test [grc_control_test] table and related support data in the Control Test Definition [grc_control_test_definition] table (extension of sysauto_script).
GRCControlAppliesToTableSetter	Displays results in an array of table names defined in the com.snc.governance.control_applies_to_tables property, which limits the list to those tables available in the Applies to field on the Control form.
GRCSurveySubmit	Handles submission of the survey creation form from an GRC control test definition.
GRCUpdater	Handles the update process for GRC from the UCF staging tables.
JSON Parser	Parses a JSON string to a Javascript object.
SetGRCRiskApproach	Handles the setting of the risk approach and the resulting risk calculation.
SetObservationItemTables	Called by the tableChoicesScript attribute on the grc_observation_affected_item.table field.
UCFDownloader	Downloads UCF content into staging tables.
VersionControlHelper	Manages versions for certain GRC objects.

Client scripts installed with Governance, Risk, and Compliance (GRC) - Legacy

Governance, Risk, and Compliance (GRC) adds the following client scripts.

Table 74: Client Scripts

Name	Table	Description
Assignment Group Changes	Observation [src_observation]	When the Assignment group is changed, clears the Assigned to field.
Authority Document Changes	Observation [src_observation]	When the Authoritative source field changes, clears the Content reference and Content category fields.
Condition Type Basic	Control Test Definition [grc_control_test_definition]	Manages the fields displayed when the Condition type field changes.
Empty name field	Control [grc_control]	Clears the Name field.
Hide Recipients on dynamic		
Hide survey macro onload	Control Test Definition [grc_control_test_definition]	Hides attestations when the Control Test Definition page is loaded.
Include Supporting Data is false	Control Test Definition [grc_control_test_definition]	Clears related fields when the "Supporting data" field is false.
Refocus on Relationship	Authoritative Source Content Mapping [m2m_auth_scr_con_auth_scr_con]	Rebuilds the relationship between two citation records on page load.
Require Method when Active - State	Control Test Definition [grc_control_test_definition]	Checks the value in the State field of a control test definition and requires users to select a Method when the state is Active.
Require Method when Active - validating	Control Test Definition [grc_control_test_definition]	Checks the Method field of a control test definition for a value when the State field is Active.
Set active flag	Control Test Definition [grc_control_test_definition]	Sets the Active flag so that the UI policies run correctly. This business rule is designed to run onLoad so that the active and state fields are synchronized.
Show User field on "Create"		
Submit Survey First	Control Test Definition [grc_control_test_definition]	Submits the attestation as a survey when saving a control test definition.
Update table on template change	Control Test Definition [grc_control_test_definition]	Updates the Table field in the control test definition record when the filter for the selected template changes.

## Business rules installed with Governance, Risk, and Compliance (GRC) - Legacy

Governance, Risk, and Compliance (GRC) adds the following business rules.

Table 75: Business Rules

Name	Table	Description
Add control test def to audit def	Audit Definition Requirement [m2m_audit_def_requirement]	Creates records in the control test definition related list when a control test is associated with the requirement.
Add control test definition to audit	Requirements [grc_audit_requirements]	Creates records in the control test definition related list when a supporting control is associated with the requirement.
Add control test to audit	Requirements [grc_audit_requirements]	Creates records in the control test related list when a supporting control is associated with the requirement.
Associate to Audit	Control Test [grc_control_test]	Creates records to associate an audit with a control test.
Calculate GRC Links	Policy Authority Documents [m2m_policy_authoritative_source]	Rebuilds calculated links between authority document and policy records.
Calculate GRC Links	Control Citation [m2m_control_auth_scr_content]	Rebuilds calculated links between citation and control records.
Calculate GRC Links	Risk Control [m2m_risk_control]	Rebuilds calculated links between risk and control records.
Calculate GRC Links	Risk Policy [m2m_risk_policy]	Rebuilds calculated links between risk and policy records.
Calculate GRC Links	Policy Control [m2m_control_policy]	
Calculate GRC Links	Policy Citation [m2m_policy_auth_src_content]	Rebuilds calculated links between citation and policy records.
Calculate GRC Links	Control Authority Document [m2m_control_authoritative_source]	Rebuilds calculated links between authority document and control records.
Calculate GRC Links	Citation [grc_authoritative_src_content]	Rebuilds calculated links between citation and related records.
Calculate GRC Links	Risk Authority Document [m2m_risk_authoritative_source]	Rebuilds calculated links between authority document and risk records.



Name	Table	Description
Cancel GRC control test workflow	Control Test [grc_control_test]	Notifies a control test assignee that a control test has been canceled.
Cancel rest of instances when one done	Control Test [grc_control_test]	Manages the states of control test definitions when attestations are completed or closed.
Change GRC Property	System Property [sys_properties]	Reruns the filter and differences if the <code>ignore_changes_to_modified_date</code> property changes.
Check reference before delete AS	Authority Document [grc_authoritative_source]	Checks versioning references before deleting authority documents.
Check reference before delete ASC	Citation [grc_authoritative_src_content]	Checks versioning references before deleting citations.
Check reference before delete control	Control [grc_control]	Checks versioning references before deleting controls.
Create New Control Version	Control [grc_control]	Creates a new control version instead of a new document.
Create New GRC Auth Source Version	Authority Document [grc_authoritative_source]	Creates a new authority document version instead of a new document.
Create New GRC Auth Src Content Version	Citation [grc_authoritative_src_content]	Creates a new citation version instead of a new document.
Create Policy Control Record	Risk Control [m2m_risk_control]	Creates a relationship from a control to a risk for every control that is related to that risk, if the relationship does not already exist.
Create Policy Control Record	Risk Policy [m2m_risk_policy]	Creates a relationship from a risk to a policy for every policy that is related to that risk, if the relationship does not already exist.
Create Policy to Auth Src Record	Policy Citation [m2m_policy_auth_src_content]	Creates a relationship from a policy to an authority document for every policy that is related to that authority document, if the relationship does not already exist.
Create Remediation on Failure	Control Test [grc_control_test]	Creates a remediation record when the control test is set to failed.

Name	Table	Description
Delete control tests in auth src	Control [grc_control]	Removes the link from control tests to an authority document when a control is deleted.
Delete Policy Control Record	Risk Control [m2m_risk_control]	Removes the records that link a control to a risk.
Delete Policy Control Record	Risk Policy [m2m_risk_policy]	Removes the records that link a policy to a risk.
Delete test in policy	Control [grc_control]	Updates policies related to a control when the control is deleted.
Delete test in risk	Control [grc_control]	Updates risks related to a control when the control is deleted.
Empty name field	Control [grc_control]	Manages an empty control name field.
Execute from Audit	Control Test Definition [grc_control_test_definition]	Executes a control test definition when its Audit Source field changes.
getColumnnsFromTable	Global [global]	
getControlTestsByDefinition	Global [global]	
getControlTestsForAudit	Global [global]	
getRelatedTestDefinitions	Global [global]	Returns control test records by their definition.
getRelatedTests	Global [global]	Returns all control test definitions associated to the citation record.
Insert Rule	Control Test Definition [grc_control_test_definition]	Creates a new control test definition ID when a control test definition is created.
Insert test in control definition delete	Control Test [grc_control_test]	Updates control test definitions when a control test is deleted.
Insert test status in control definition	Control Test [grc_control_test]	Updates control test definitions when a new control test
Notify assessment user	Assessment Instance [asmt_assessment_instance]	Notifies an assessment user that an assessment is ready to take.
Notify control test assignee	Control Test [grc_control_test]	Notifies an assignee when a control test is assigned.
Require a valid method when active	Control Test Definition [grc_control_test_definition]	Selects an assignment method to activate this control test definition.

Name	Table	Description
Rollup summary to authoritative document	Control [grc_control]	Updates the authority document rollup summaries when a control passes or fails.
Rollup summary to control	Control Test Definition [grc_control_test_definition]	Updates the control rollup summaries when a control test definition passes or fails.
Rollup summary to control delete	Control Test Definition [grc_control_test_definition]	Updates the control rollup summaries when a control test definition is deleted.
Rollup summary to policy	Control [grc_control]	Updates the policy rollup summaries when a control test definition is deleted.
Rollup summary to policy	Policy Control [m2m_control_policy]	Updates the policy rollup summaries when a relationship between a control and a policy is deleted.
Rollup summary to risk	Control [grc_control]	Updates the risk rollup summaries when a control test definition is deleted.
Rollup summary to risk m2m	Risk Control [m2m_risk_control]	Updates the risk rollup summaries when a relationship between a control and a risk is deleted.
Set active flag	Control Test Definition [grc_control_test_definition]	Updates the "Active" field based on a status change.
Set attestation columns	Control Test Definition [grc_control_test_definition]	Sets default values related to attestations when a control test definition is created or updated.
set compliant flag	Requirements [grc_audit_requirements]	Sets the Compliant field when an audit requirement state is changed.
Set point in time sample data value	Control Test [grc_control_test]	Adjusts the control test sample data time when the status is changed
Setting name to reference if no name	Citation [grc_authoritative_src_content]	Updates a citation's Name field if an authority document reference name is changed.
Store attestation results	Assessment Instance [asmt_assessment_instance]	Updates attestation results when assessment instance data is modified.
Sync columns to metric type table	Control Test Definition [grc_control_test_definition]	Updates assessment metric tables when an attestation is created or updated in a control test definition.

Name	Table	Description
Sync intro to control test definition	Assessment Metric Type [asmt_metric_type]	Updates an attestation introduction in a control test definition when the assessment metric type is updated.
Sync name and reference	Citation [grc_authoritative_src_content]	
Update assign to user and group	Control Test Definition [grc_control_test_definition]	Manages the "Assigned to" and "Assigned to group" fields when the "Method" field is updated.
Update auth src count in control	Control Authority Document [m2m_control_authoritative_source]	Manages the count of controls linked to an authority document.
Update auth src count in controls	Authority Document [grc_authoritative_source]	Manages the count of authority documents linked to a control.
Update control coverage	Control Authority Document [m2m_control_authoritative_source]	Updates coverage values in authority documents based on the status of linked controls.
Update control coverage from def delete	Control Test Definition [grc_control_test_definition]	Updates coverage values in controls based on the deletion of linked control test definitions.
Update control coverage from definition	Control Test Definition [grc_control_test_definition]	Updates coverage values in controls based on the creation or modification of linked control test definitions.
Update control tests in auth src	Control Authority Document [m2m_control_authoritative_source]	Update links between an authority document and its controls when link table records are created, updated or deleted.
Update coverage on control active	Control [grc_control]	Updates coverage values in an authority document based on the creation or modification of linked controls.
Update coverage on control delete	Control [grc_control]	Updates coverage values in an authority document based on the deletion of linked controls.
Update duration in control test def	Assessment Metric Type [asmt_metric_type]	Updates a control test definition's Duration field when an attestation instance's duration has changed.
Update Pertinent Flag	Risk Authority Document [m2m_risk_authoritative_source]	Updates the Pertinent flag for the link table between a risk and an authority document.
Update Pertinent Flag	Policy Citation [m2m_policy_auth_src_content]	Updates the Pertinent flag for the link table between a policy and citations.

Name	Table	Description
Update Pertinent Flag	Policy Control [m2m_control_policy]	Updates the Pertinent flag for the link table between a policy and controls.
Update Pertinent Flag	Policy Authority Document [m2m_policy_authoritative_source]	Updates the Pertinent flag for the link table between a policy and an authority document.
Update Pertinent Flag	Risk Policy [m2m_risk_policy]	Updates the Pertinent flag for the link table between a policy and a risk.
Update Pertinent Flag	Control Authority Document [m2m_control_authoritative_source]	Updates the Pertinent flag for the link table between a control and an authority document.
Update Pertinent Flag	Policy Citation [m2m_policy_auth_src_content]	Updates the Pertinent flag for the link table between a policy and a citation.
Update Pertinent Flag	Control Citation [m2m_control_auth_src_content]	Updates the Pertinent flag for the link table between a control and a citation.
Update Pertinent Flag	Risk Control [m2m_risk_control]	Updates the Pertinent flag for the link table between a risk and a control.
Update pertinent GRC Links	Control [grc_control]	Updates the Pertinent flag for a control.
Update pertinent GRC Links	Citation [grc_authoritative_src_content]	Updates the Pertinent flag for a citation.
Update pertinent GRC Links	Authority Document [grc_authoritative_source]	Updates the Pertinent flag for an authority document.
Update pertinent GRC Links	Policy [grc_policy]	Updates the Pertinent flag for a policy.
Update pertinent GRC Links	Risk [grc_risk]	Updates the Pertinent flag for a risk.
Update policy count in control	Policy Control [m2m_control_policy]	Updates the Policy count field for the link table between a policy and a control.

## Activate GRC Risk - Legacy

Administrators can activate the GRC: Risk plugin [com.sn\_risk] and doing so automatically installs the Core GRC Components [com.snc.governance\_core] plugin. Additional plugins are activated as needed. This plugin provides demonstration data.

**Note:** The Core GRC Components [com.snc.governance\_core] plugin includes components used by the Governance, Risk, and Compliance (GRC) [com.snc.governance] plugin, the GRC: Risk plugin [com.sn\_risk], and the Security Incident Response GRC support plugin

[com.snc.security\_incident.grc] plugin. These components include GRC Risks, Risk Criteria, Remediation Tasks, Policies, Standards, and Standard Operating Procedures.

1. Navigate to System Definition Plugins .
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

If the plugin has optional features that are not functional because other plugins are inactive, those plugins are listed. A warning states that some files are not installed. If you want the optional features to be installed, cancel this activation, activate the necessary plugins, and then return to activating the plugin.

4. If available, select the Load demo data check box.

Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.

5. Click Activate.

## Components installed with GRC: Risk - Legacy

Several types of components are installed with the GRC: Risk plugin.

Demo data is available with GRC: Risk.

## Tables installed with GRC: Risk - Legacy

GRC: Risk adds the following tables.

Name	Description
Risk Definition [sn_risk_definition]	Stores definitions of risks.
Profile Type to Risk Definition [sn_risk_m2m_definition_profile_type]	Stores many to many relationship between risk definitions and profile types.

---

**Note:** All additional tables installed by the dependent plugins are also needed for GRC: Risk.

---

## Properties installed with GRC: Risk - Legacy

GRC: Risk adds the following properties.

Name	Description
com.snc.grc_risk.max_significance	Sets the maximum value for Risk Significance. Out-of-box the value is set at 5, but it can be a whole number in-between 1-10.
com.snc.grc_risk.max_likelihood	Sets the maximum value for Risk Likelihood. Out-of-box the value is set at 5, but it can be a whole number in-between 1-10.

## Roles installed with GRC: Risk - Legacy

GRC: Risk adds the following roles.

**Table 76: Installed user roles**

Name	Description
Admin [sn_risk.admin]	<ul style="list-style-type: none"> <li>• Provides administrative rights to the Risk application and modules.</li> <li>• Has all the rights of a sn_risk.manager and a sn_risk.user, as well as the ability to define Risk Criteria and set Risk Criteria Thresholds and risk Properties.</li> <li>• Inherits the following roles.               <ul style="list-style-type: none"> <li>• sn_grc.admin</li> <li>• sn_grc.manager</li> <li>• sn_grc.user</li> <li>• sn_risk.manager</li> <li>• sn_risk.user</li> </ul> </li> <li>• Inherits the following roles if the Governance, Risk, and Compliance (GRC) application is activated.               <ul style="list-style-type: none"> <li>• grc_audit_reader</li> <li>• task_editor</li> <li>• certification_admin</li> <li>• grc_test_definition_admin</li> <li>• grc_control_test_reader</li> <li>• assessment_admin</li> <li>• certification</li> <li>• grc_compliance_reader</li> <li>• certification_filter_admin</li> <li>• grc_admin</li> <li>• grc_user</li> </ul> </li> </ul>

Name	Description
Manager [sn_risk.manager]	<ul style="list-style-type: none"> <li>• Provides management rights to the Risk application and modules.</li> <li>• Has all the rights of a sn_risk.user as well as the ability to create new Profile Types, Profiles, and Risk Definitions, and has access to the Risk Overview.</li> <li>• Has the ability to manage assessments.</li> <li>• Inherits the following roles. <ul style="list-style-type: none"> <li>• sn_grc.manager,</li> <li>• sn_grc.user</li> <li>• sn_risk.user</li> </ul> </li> <li>• Inherits the following roles if the Governance, Risk, and Compliance (GRC) application is activated. <ul style="list-style-type: none"> <li>• grc_audit_reader</li> <li>• task_editor</li> <li>• certification_admin</li> <li>• grc_test_definition_admin</li> <li>• grc_control_test_reader</li> <li>• assessment_admin</li> <li>• certification</li> <li>• grc_compliance_reader</li> <li>• certification_filter_admin</li> <li>• grc_user</li> </ul> </li> </ul>
User [sn_risk.user]	<ul style="list-style-type: none"> <li>• Provides access rights to the Risk application and modules. Can view Profile Types, Profiles, Risks, and Remediation tasks.</li> <li>• Can create and manage new and existing Risks. Cannot view Risk Definitions, create new Profiles or Profile Types, and does not have access to the Risk Overview.</li> <li>• Inherits the sn_grc.user role.</li> <li>• Inherits the following roles if the Governance, Risk, and Compliance (GRC) application is activated. <ul style="list-style-type: none"> <li>• grc_compliance_reader</li> <li>• grc_user</li> <li>• grc_audit_reader</li> <li>• grc_control_test_reader</li> <li>• task_editor</li> </ul> </li> </ul>

Script includes installed GRC: Risk - Legacy

GRC: Risk adds the following script includes.



Name	Description
RiskUtilsBase	Provides base risk utilities. Protected script include which cannot be edited by client.
RiskUtils	Editable script include so that RiskUtilsBase can be overridden without affecting the base code.
RiskUtilsAJAX	Client callable risk methods.

## Business rules installed with GRC: Risk - Legacy

GRC: Risk adds the following business rules.

Name	Table	Description
Rollup Profile Scores	Profile [sn_grc_profile]	Calculates inherent, residual, and calculated risk scores from the likelihood and significance of all risks associated with a profile.
Assign risks to profiles	Profile [sn_grc_profile]	Allows the system to assign risks to various profiles.
Rollup Profile Scores	Risk [grc_risk]	Calculates inherent, residual, and calculated risk scores from the likelihood and significance of all risks associated with a profile.
Calculate Scores	Risk [grc_risk]	Calculates the inherent, residual, and calculated risk score from the likelihood and significance of a risk.
Update applies to when profile changes	Risk [grc_risk]	Updates the 'applies to' field on the risk form when the profile is changed on the risk form.

## Plugins installed with GRC: Risk - Legacy

GRC: Risk adds the following plugins.

Plugin Name	Plugin ID	Description
GRC: Risk	com.sn_risk	Enables core Risk Management functionality. Installs GRC: Profile.
GRC: Profiles	com.sn_grc	Enables core GRC profile functionality and associated components.
Governance, Risk, and Compliance Core	com.snc.governance_core	Provides the core Risk and Policy functionality used by GRC.

Plugin Name	Plugin ID	Description
Assessment	com.snc.assessment_core	Loads the ServiceNow assessment engine, which powers GRC attestations. Attestations created in GRC use assessment tables and can be customized using the Assessment application.
Certification Core	com.snc.certificaiton_core	Provides all core compliance functionality, including certification templates used by GRC to create control test definitions.

## What is GRC? - Legacy

Governance, risk, and compliance (GRC) is a general term describing the combination of people, processes, and products involved in establishing and executing business goals, while mitigating risk and proving compliance with regulations.

The Governance, Risk, and Compliance (GRC) application supports:

- Creating policies
- Defining and assessing risks
- Defining controls based on policies and their associated risks
- Downloading and importing Unified Compliance Framework (UCF) data. See <https://www.unifiedcompliance.com/>.
- Generating audits and tests to ensure that controls are being followed
- Generating remediation tasks to track corrective actions that are required

## GRC functional and technical roles - Legacy

These roles provide access to Governance, Risk, and Compliance (GRC) and can perform all the activities of the roles they contain.

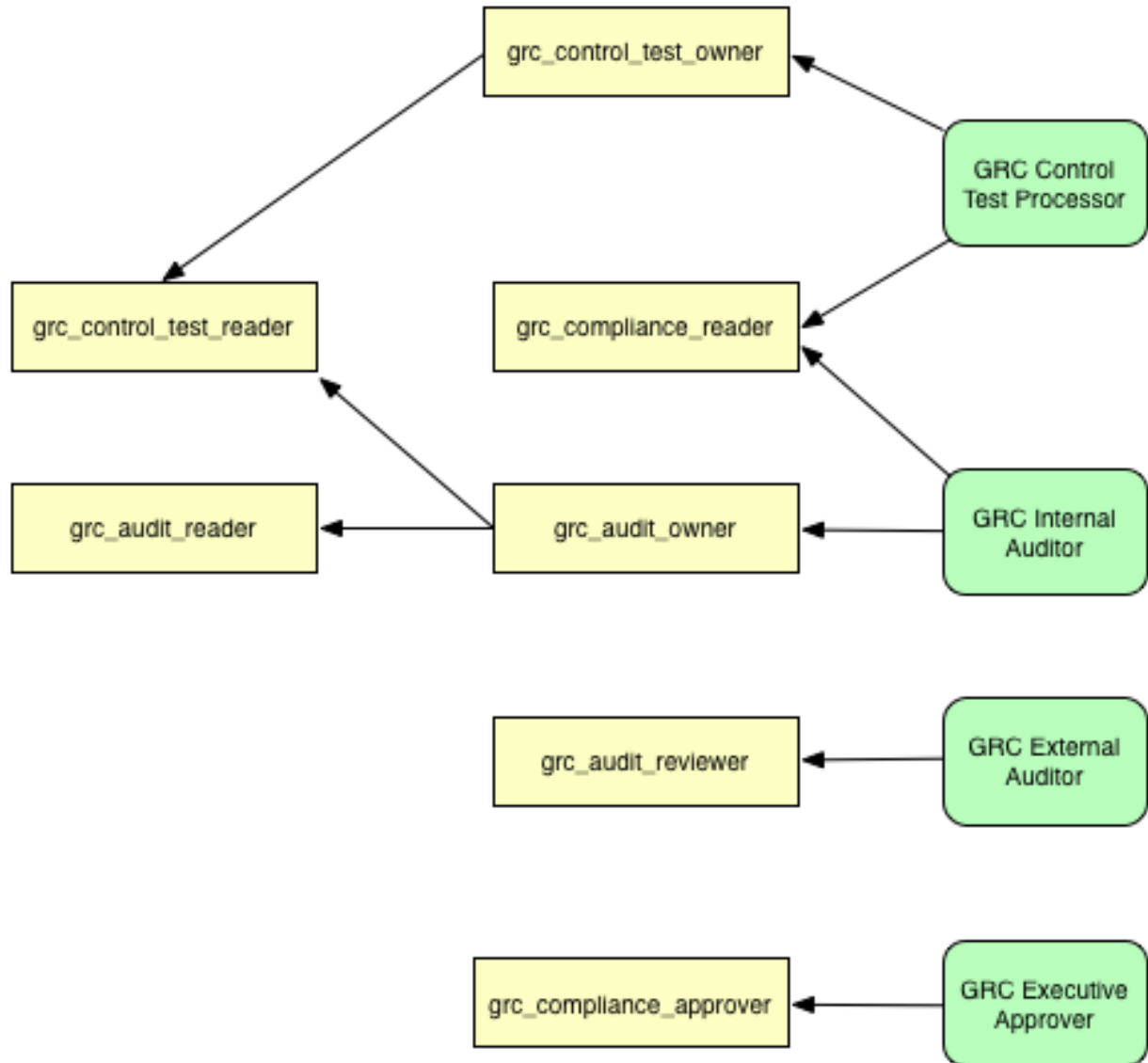
Functional roles provide general compliance capabilities to users in the system. Grant these roles to auditors, approvers, and users who manage control tests. These roles can be modified to suit an organization's needs.

Technical roles provide specific capabilities to users in the system and when combined create functional roles.

---

**Note:** Users with the ITIL role have access to the application and can edit control tests, remediation tasks, and audits.

---



**Figure 6: GRC technical and functional roles**

## GRC administration and configuration - Legacy

The GRC Administration module provides administrative- and configuration-type functions for users with administrative roles assigned to them.

## UCF import properties - Legacy

The preconfigured values in the UCF import properties define the connection specifics for the UCF source documents and should not be changed.

To view UCF properties, navigate to [GRC Administration Properties](#).

Table 77: UCF import properties

Label	Name	Description
URL of UCF website	com.snc.governance.url	Address of the UCF website. The file path to the UCF XML file is appended to this URL. The default provided by the ServiceNow system is http://www.unifiedcompliance.com.
User of UCF website account	com.snc.governance.user	User name for the UCF account that has access to the downloaded files. By default, the value in this property is blank. The ServiceNow system provides a UCF account user that is coded into the system. If you have your own UCF account, enter the user name to override the one provided by the ServiceNow system.
Password of UCF website account	com.snc.governance.password	Password for the UCF account that has access to the download files. By default, the value in this property is blank. The ServiceNow system provides a UCF account password for its configured user. If you have your own UCF account, enter the password in this property to override the one provided by the ServiceNow system.
File path relative to UCF URL	com.snc.governance.path	Path to the specified download file on the UCF server. This path is provided by the ServiceNow system and is appended to the address for the UCF website and names the authoritative document to download. This path downloads the latest version of the UCF XML file and does not need to be changed.

## Configure GRC update to ignore date change - Legacy

GRC only creates new versions of authority documents, citations, and controls if those entities have changed in downloaded UCF documents.

By default, the system ignores changes to the *last modified date* of a UCF document when creating a new version. To allow GRC to create new versions of documents whose dates have changed:

1. Navigate to GRC > Administration > Properties .
2. Clear the check box for the Ignore changes to UCF modified date property.

3. Click Save.

## Define GRC scope - Legacy

Scope is the effective level to which a policy, standard, or SOP applies. For example, you might apply a standard at the company level and then create an SOP for an organizational unit within the company. You define entities using these types in the Scope [grc\_entity] table and apply them to a policy class in the Scope related list.

1. Navigate to GRC Administration Scopes .
2. Click New.
3. Fill in the fields on the form, as appropriate:

**Table 78: Scope**

Field	Description
Name	Enter a unique and descriptive name for the scope.
Type	Select a type <ul style="list-style-type: none"> <li>• Location</li> <li>• Business Area</li> <li>• Operational Classification</li> </ul>

4. Click Submit.

## Create or modify a risk criteria threshold - Legacy

Risk Criteria are the scoring values attributed to the likelihood that a risk will occur, and the significance to your organization if the risk does occur. Risk Criteria Thresholds allow you to define what is deemed a high/likely or low/unlikely score. You can create or modify risk criteria thresholds, as necessary.

Risk defines Risk Criteria Thresholds as follows.

**Table 79: Risk Criteria Thresholds**

Likelihood	Significance	Scores
1 = Extremely Unlikely	1 = Very Low	0-5 = Very Low
2 = Unlikely	2 = Low	6-10 = Low
3 = Neutral	3 = Moderate	11-15 = Moderate
4 = Likely	4 = High	16-20 = High
5 = Extremely Likely	5 = Very High	21-25 = Very High

---

**Note:** See [Risk scoring](#) for information how the scores of Risks are calculated.

---

1. Navigate to Risk Administration Risk Criteria Thresholds .
2. Select the threshold to modify or click New.
3. Fill in the fields on the form, as appropriate.

Name	Description
Label	Sets the name of the Risk Criteria Threshold (for example, Extremely Likely or Very Low).
Type*	Select Likelihood, Significance, or Score depending on which the new threshold will apply.
Max value*	Sets the max score for a threshold.  <b>Note:</b> The properties restrict the values of Likelihood and Significance to 1-10. Therefore it is not beneficial to create Likelihood or Significance thresholds for max values greater than 10 or Score thresholds for max values greater than 100.

**Note:** \* indicates a mandatory field.

4. Click Submit.

## GRC condition collections in control test definitions - Legacy

Condition collections have one primary condition, which is applied to the selected table, and one or more supplemental conditions. Set the Condition type to Advanced on control tests to define more flexible conditions using condition collections.

When a control test is performed, advanced conditions evaluate in this order:

1. The system processes the condition collection in the In scope definition reference in this order:
  - The primary condition is processed on the fields specified in Table and Fields on the control test definition, returning an array of elements.
  - For each element in the array returned by the primary condition, supplemental conditions are processed, filtering the array of elements further.
  - The In scope definition field is updated with the number of elements in the array.
2. The condition collection in the Configuration reference is processed on the array of elements returned from the In scope definition. The choices for Configuration to retrieve are:

**Table 80: Choices for Configuration to retrieve**

Choice	Description
None	These conditions are skipped. Supporting Data is all of the elements that are in scope.
Matching	The control test checks the array of elements, returning any elements that match the Configuration.
Non-Matching	The control test checks the array of elements, returning any elements where at least one condition did not match the Configuration.

- The final array of elements is recorded as Supporting data records.

---

**Note:** Both the In scope definition and Configuration fields refer to the Condition Collection [grc\_condition\_collection] table.

---

*Create a condition for a GRC condition collection - Legacy*

Create the conditions to use in a control test definition condition collection.

- Navigate to GRC Administration Conditions .
- Click New.
- Fill in the fields on the form, as appropriate.

**Table 81: Condition form fields**

Field	Description
Name	Name of the condition or of the condition collection in which it appears.
Description	Description of the condition or the condition collection in which it appears.
Table	Table on which the condition is applied.
Reference field	For supplemental conditions, the reference field for the table on which the primary condition is running.
Condition	Condition builder for defining the condition.

*Create a GRC condition collection - Legacy*

Create a condition collection with primary and supplemental conditions.

- Navigate to GRC Administration Condition Collections .
- Click New.
- Fill in the fields on the form, as appropriate.

**Table 82: Condition form fields**

Field	Description
Name	Name of the condition collection.
Description	Description of the condition collection.
Type	Which Control Test Definition field references the condition collection. Your choices are: <ul style="list-style-type: none"> <li>In Scope Definition</li> <li>Configuration Definition</li> </ul>

- After the condition collection is defined, use the Add Condition related link to add these conditions:
  - Condition: Predefined condition definition from the Condition [grc\_condition] table.
  - Condition type: Choices are determined by the condition collection Type:

- In Scope Definition
- Primary
- Supplemental
- Configuration Definition
- Not Applicable

## Create a GRC control test definition - Legacy

A control test definition determines how and when a control test is performed, including execution steps and expected results. Condition collections can be created with associated conditions to define advanced control test logic. Each time the control test is performed, a control test instance is generated as a task to be executed, according to the control test definition. After you define a control, create control tests to gather documented evidence of whether the associated control is operating correctly.

When you configure a control test definition to provide supporting data , you can select different methods of gathering that data.

1. Navigate to GRC Administration Control Test Definitions .
2. Click New.
3. Fill in the top part of the form, as appropriate.
4. Click Submit to save the record or Execute now to save and execute this control test definition.



<
Control Test Definition
>

Definition ID:

\* Name:

Duration: Days  Hours

\* Method:

\* Assign to:

State:

Control:

Remediation group:

Escalate task:

Run:

Day:

Time: Hours

Execution step:

Expected result:

Collect supporting data:

Table 83: Control test definition fields

Field	Description
Definition ID	A unique identifier generated dynamically by the system.
Name	The name of the control test.
Duration	Defines the due date for an attestation or the elapsed time until this control test is marked passed or failed. For attestations, you can configure the duration in this form or in the Assessment Metric Type form. For recipient notification, If the duration is at least two days, the system deducts one day from the duration when notifying recipients of milestones. This allows time to review the attestation results before the due date expires. The default duration is 14 days.
Method	One of the following choices for determining the test assignee: <ul style="list-style-type: none"> <li>Assign to Group: Assignment group for the control test.</li> <li>Assign to Individual: User assigned to the control test.</li> </ul>
Assign to group	Group assigned to this control test. This field is available only when the selected method is Assign to Group.
Assign to	User assigned to this control test. The choice list is limited to users whose role permits them to view and score control tests. This field is available only when the selected method is Assign to Individual.
State	A workflow field that indicates the state of the drafting process for this control test definition. If the state is Active, control test instances are dynamically generated based on this record's definition. A control test definition must be active before it can be executed.
Control	A reference to the control being enforced. <p><b>Note:</b> <i>Do not</i> change the control in this record after the control test instance has been generated. If you need to change the control, create a new control test definition with the same settings and then select the new control.</p>

Field	Description
Remediation group	Group assigned to the remediation tasks if a control test fails.
Escalate task	Check box to escalate the priority of the control test associated with this control test definition as the due date approaches. The escalation schedule is: <ul style="list-style-type: none"> <li>• Low: 0% - 50%</li> <li>• Moderate: 50% - 90%</li> <li>• High: 90% - 100%</li> <li>• Critical: Overdue</li> </ul>
Run	Frequency for generating control test instances. Choices are: <ul style="list-style-type: none"> <li>• Daily</li> <li>• Weekly</li> <li>• Monthly</li> <li>• Periodically</li> <li>• Once</li> <li>• On Demand</li> </ul>
Day	Day of the week that a control test instance is generated each week if Run is set to Weekly. Day of the month if Run is set to Monthly.
Time	The time that a control test instance is automatically generated if "Run" is set to "Daily", "Weekly", "Monthly", or "Periodically".
Repeat interval	A duration, in days and hours, between the automatic generation of control test instances if Run is set to Periodically.
Starting	The date and time control test instances are first generated if Run is set to Periodically. The only date and time a control test instance is generated if Run is set to Once.
Execution step	Description of this step in the process of satisfying the control. For example, if you are administering an attestation, the step might be to collect attestations and evaluate the results.
Expected result	The result that should occur after these tests. Describe how the results of test are used to support the control.

Field	Description
Collect supporting data	Indicator whether sample data should be taken from a particular table within the instance when the control test instance is generated. Select this check box to display additional fields for supporting data.

## Add supporting data to a GRC control test definition - Legacy

Supporting data in a control test definition displays the Condition type field.

Each condition gathers data using a different combination of fields.

1. Click Collect supporting data.
2. Select a condition type:

**Table 84: Condition types**

Condition type	Description
Basic	Applies specific conditions to the table specified.
Advanced	Uses condition collections to apply conditions to the table and to related tables.
Template	Uses certification templates to apply conditions to the table specified.
Attestation	Uses surveys administered to users and groups to collect data.

## Define an advanced condition in a GRC control test definition - Legacy

Advanced condition types apply conditions to the table and to related tables with condition collections.

1. In the Control Test Definition form, click Collect supporting data.
2. Select Advanced from the choice list.
3. Fill in the fields on the form, as appropriate:

Collect supporting data

\* Condition type

\* Data purpose

\* Table

\* Fields

\* In scope definition

Configuration to retrieve

Configuration

**Table 85: Advanced condition fields**

Field	Description
Data purpose	<p>Purpose of the data being sampled. This selection influences how the control test is performed. Choices are:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Support test execution: Returns a random sampling of records.</li> <li>• Identifies non compliance: Returns all of the records that do not match the condition or conditions specified.</li> <li>• Identifies compliance: Returns all of the records that do match the condition or conditions specified.</li> </ul>

Field	Description
Table	Table from which to collect the data. This field is read-only when Template is the Condition type. When you select a template to define test conditions, the table is set by the certification filter used in the template and cannot be changed.
Fields	List of fields whose values you want to evaluate when determining whether records match the conditions.
In scope definition	Reference to a condition collection. For more information see Defining Advanced Conditions.
Configuration to retrieve	Method for using the Configuration reference field. Possible choices are: <ul style="list-style-type: none"> <li>• None: Returns all records in scope.</li> <li>• Matching: Returns all matching records in scope.</li> <li>• Non-matching: Returns all non-matching records in scope.</li> </ul>
Configuration	Condition collections to use. This field is available only if Configuration to retrieve is set to anything except None.

## Define a basic condition in a GRC control test definition - Legacy

Basic condition types apply specific conditions to the table specified.

1. In the Control Test Definition form, click Collect supporting data.
2. Select Basic from the choice list.
3. Fill in the fields on the form, as appropriate:

Collect supporting data

\* Condition type

\* Data purpose

\* Table

\* Fields

\* Sample size

Control test condition

**Table 86: Basic condition fields**

Field	Description
Data purpose	<p>Purpose of the data being sampled. This selection influences how the control test is performed. Choices are:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Support test execution: Returns a random sampling of records.</li> <li>• Identifies non compliance: Returns all of the records that do not match the condition or conditions specified.</li> <li>• Identifies compliance: Returns all of the records that do match the condition or conditions specified.</li> </ul>
Table	<p>Table from which to collect the data. This field is read-only when Template is the Condition type. When you select a template to define test conditions, the table is set by the certification filter used in the template and cannot be changed.</p>

Field	Description
Fields	List of fields whose values you want to evaluate when determining whether records match the conditions.
Sample size	An integer number of rows for a random sample. A sample size of zero returns all matching records. This field is available only if Data purpose is set to Support test execution.
Control test condition	A condition builder that limits the sample data. This field is available only if Condition type is set to Basic.

## Define a template condition in a GRC control test definition - Legacy

Template conditions use certification templates to apply conditions to the specified table.

1. In the Control Test Definition form, click Collect supporting data.
2. Select Template from the choice list.
3. Fill in the fields on the form, as appropriate:

Collect supporting data

\* Condition type

\* Data purpose

\* Table

\* Fields

Configuration to retrieve

\* Template



Table 87: Advanced condition fields

Field	Description
Data purpose	<p>Purpose of the data being sampled. This selection influences how the control test is performed. Choices are:</p> <ul style="list-style-type: none"> <li>• None</li> <li>• Support test execution: Returns a random sampling of records.</li> <li>• Identifies non compliance: Returns all of the records that do not match the condition or conditions specified.</li> <li>• Identifies compliance: Returns all of the records that do match the condition or conditions specified.</li> </ul>
Table	<p>Table from which to collect the data. This field is read-only when Template is the Condition type. When you select a template to define test conditions, the table is set by the certification filter used in the template and cannot be changed.</p>
Fields	<p>List of fields whose values you want to evaluate when determining whether records match the conditions.</p>
Configuration to retrieve	<p>Method for using the Configuration reference field. Possible choices are:</p> <ul style="list-style-type: none"> <li>• None: Returns all records in scope.</li> <li>• Matching: Returns all matching records in scope.</li> <li>• Non-matching: Returns all non-matching records in scope.</li> </ul>
Template	<p>[Required] Certification template that defines conditions for this test definition. Only templates with an audit type of Compliance are available for selection. This field is available and mandatory when the value in the Condition type field is Template.</p>

## Create a GRC audit definition - Legacy

An audit definition establishes a set process for validating controls and control tests. From the definition, audit instances can be generated as a task to power the audit.

1. Navigate to GRC Administration Audit Definitions .
2. Click New.
3. Fill in the fields on the form, as appropriate.

Field	Input Value
ID	A unique ID for the audit definition, populated by Number Maintenance.
Name	A name for the audit definition.
Owning group	A reference to a group to have ownership over the audit process.
Owner	A reference to a user to have ownership over the audit process.
Execution group	A reference to the group that will execute the audit.
Type	The type of audit process.
State	Where in the drafting process the definition is.
Short description	A short description of the audit.
Description	A full description of the audit.

4. Use the related list Control Test Definitions to specify control tests to perform during the audit.
5. Use the related list Scope to define entities for the audit to refer to.

## Define GRC risk criteria - Legacy

Use the Risk Criteria form to define risk criteria.

In the base GRC system, the risk criteria available on the form are Significance and Likelihood.

1. Navigate to GRC Administration Risk Criteria .
2. Click New.
3. Fill in the fields on the form, as appropriate:

**Table 88: Risk criteria fields**

Field	Description
Type	Select one of the types provided, either Likelihood or Significance.
Display value	Create a name for the criteria that displays in the choice list. For example, enter 3 - Expected Behavior for the Likelihood type.
Order	The order in which this choice appears in the choice list. This order should be logical for the level selected.
Weighting	A numeric value for the risk, used to calculate risk approach rules. Low weighting factor indicates a lower overall risk, and high weighting factor indicates a higher overall risk.

4. Click Submit.

5. To select the new criteria in a risk record, navigate to **GRC Risks** and click **New**.
6. Open the choice list for the **Likelihood** field.

The new criteria appears in the list by its display name.

The screenshot shows a ServiceNow form for a Risk record. The form has a header with a back arrow, a menu icon, and the title "Risk". The fields are as follows:

- Risk ID:** RISK0002002
- \* Name:** (empty text field)
- Significance:** -- None --
- Likelihood:** -- None -- (dropdown menu is open, showing options: -- None --, 5 - Extremely Likely, 4 - Improbable, 3 - Expected Behavior, 4 - Unexpected, 2 - Unknown, 1 - Unlikely. The option "3 - Expected Behavior" is highlighted in blue).
- Recommended approach:** (empty text field)
- Pertinent:** (empty text field)
- Description:** (empty text area)

## GRC reporting portals - Legacy

Users of governance, risk, and compliance can view reports on attestations, compliance, controls, and audits. The GRC reporting portals provide reports to specific users related to the GRC elements assigned to them or their groups.

GRC provides portals that deliver reports to specific users related to the GRC elements assigned to them or their groups. Those reports include the following information.

- Overview of all UCF document import activity.
- GRC related tasks and assessments assigned to the logged in user, the user's group, or people who report to the logged in user.
- Time remaining on time-sensitive GRC elements.
- GRC update approvals for the logged in user.
- Progress on tasks, including subtasks completed versus those remaining.

- Results filtered by audit, department, company, individual, type, and group.

The available portals are:

**Table 89: GRC reporting portals**

Portal	Description
My GRC	Displays all available GRC reports in the portal to users with the <code>grc_admin</code> role. These users can add or delete any report in the GRC portal.
My GRC Approvals	Displays all available approval reports in the portal to users with the <code>grc_audit_definition_admin</code> or <code>grc_internal_auditor</code> role.
My GRC Audits	Displays all available audit reports in the portal to users with the <code>grc_audit_definition_admin</code> or <code>grc_internal_auditor</code> role.
My GRC Controls	Displays all available control reports in the portal to users with the <code>grc_test_definition_admin</code> or <code>grc_process_owner</code> role.

### Available GRC reports - Legacy

This table indicates which reports are included by default in the My GRC portals and the roles required to view each portal.

Some GRC reports are driven by database views, which define table joins for reporting purposes. As with any homepage in the ServiceNow system, report gauges can be customized in these portals.

**Table 90: Available GRC reports**

Report	Description	GRC portal	Database view
Attestations by Control	<p>Displays manual attestations by controls for open control tests whose control or control test definition is owned by the logged-in user.</p> <ul style="list-style-type: none"> <li>• Type: Bar chart</li> <li>• Table: GRC Attestations by Control Test [grc_attestations_control_tests]</li> </ul>	<p>My GRC Control portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>• <code>grc_process_owner</code></li> <li>• <code>grc_test_definition_admin</code></li> </ul>	<p>grc_attestations_control_tests</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>• Assessment Instance [asmt_assessment_instance]</li> <li>• Control Test [grc_control_test]</li> </ul>

Report	Description	GRC portal	Database view
Attestations by Control (My Group)	<p>Displays manual attestations by controls for open control tests whose control or control test definition is owned by the logged-in user's group.</p> <ul style="list-style-type: none"> <li>Type: Bar chart</li> <li>Table: GRC Attestations by Control Test [grc_attestations_control_tests]</li> </ul>		<p>grc_attestations_control_tests</p> <p>Joins :</p> <ul style="list-style-type: none"> <li>Assessment Instance [asmt_assessment_instance]</li> <li>Control Test [grc_control_test]</li> </ul>
Attestations by State	<p>Displays manual attestations by state for open control tests whose control or control test definition is owned by the logged-in user.</p> <ul style="list-style-type: none"> <li>Type: Pie chart</li> <li>Table: GRC Attestations by Control Test [grc_attestations_control_tests]</li> </ul>		<p>grc_attestations_control_tests</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Assessment Instance [asmt_assessment_instance]</li> <li>Control Test [grc_control_test]</li> </ul>
Attestations by State (My Group)	<p>Displays manual attestations by state for open control tests whose control or control test definition is owned by the logged-in user's group.</p> <ul style="list-style-type: none"> <li>Type: Pie chart</li> <li>Table: GRC Attestations by Control Test [grc_attestations_control_tests]</li> </ul>		<p>grc_attestations_control_tests</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Assessment Instance [asmt_assessment_instance]</li> <li>Control Test [grc_control_test]</li> </ul>

Report	Description	GRC portal	Database view
Attestations Past Due Date	Lists overdue manual attestations for open control tests whose control or control test definition is owned by the logged-in user. <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: GRC Attestations by Control Test [grc_attestations_control_tests]</li> </ul>	My GRC Control portal Roles: <ul style="list-style-type: none"> <li>grc_process_owner</li> <li>grc_test_definition_admin</li> </ul>	grc_attestations_control_tests Joins: <ul style="list-style-type: none"> <li>Assessment Instance [asmt_assessment_instance]</li> <li>Control Test [grc_control_test]</li> </ul>
Attestations Past Due Date (My Group)	Lists overdue manual attestations for open control tests whose control or control test definition is owned by the logged-in user's group. <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: GRC Attestations by Control Test [grc_attestations_control_tests]</li> </ul>		grc_attestations_control_tests Joins: <ul style="list-style-type: none"> <li>Assessment Instance [asmt_assessment_instance]</li> <li>Control Test [grc_control_test]</li> </ul>
Audits in Progress (My Group)	Lists audits with a state of Work in Progress owned by the logged-in user's group. <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Audit [grc_audit]</li> </ul>	My GRC Audit portal Roles: <ul style="list-style-type: none"> <li>grc_audit_definition_admin</li> <li>grc_internal_auditor</li> </ul>	
Citation Coverage Gap	Displays specific citations linked to controls that are not used in any control test definition. <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: GRC ASC Coverage Gap [grc_asc_coverage_gap]</li> </ul>		grc_asc_coverage_gap Joins: <ul style="list-style-type: none"> <li>Control Authoritative Source Content [m2m_control_auth_src_content]</li> <li>Control Test Definition [grc_control_test_definition]</li> </ul>

Report	Description	GRC portal	Database view
Authority Document Coverage Gap	<p>Displays specific authority documents linked to controls that are not used in any control test definition.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: GRC AS Coverage Gap [grc_as_coverage_gap]</li> </ul>		<p>grc_as_coverage_gap</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Control Authoritative Source [m2m_control_authoritative_source]</li> <li>Control Test Definition [grc_control_test_definition]</li> </ul>
Compliance By Authority Document	<p>Displays the percentage of passing, failing, and complete control test instances from the last run for each authority document.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Authoritative Source [grc_authoritative_source]</li> </ul>	<p>My GRC portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_admin</li> <li>grc_executive_approver</li> </ul> <p>My GRC Control portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_process_owner</li> <li>grc_test_definition_admin</li> </ul>	
Compliance By Control	<p>Displays the percentage of passing, failing, and complete control test instances from the last run for each control.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Control [grc_control]</li> </ul>		
Compliance By Policy	<p>Displays the percentage of passing, failing, and complete control test instances from the last run for each policy linked to a control.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Policy [grc_policy]</li> </ul>		

Report	Description	GRC portal	Database view
Compliance By Risk	<p>Displays the percentage of passing, failing, and complete control test instances from the last run for each risk linked to a control.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Risk [grc_risk]</li> </ul>		
Controls by Authority Document	<p>Displays the count of controls for each authority document.</p> <ul style="list-style-type: none"> <li>Type: Pie chart</li> <li>Table: Control Authoritative Source [m2m_control_authoritative_source]</li> </ul>	<p>My GRC portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_admin</li> <li>grc_executive_approver</li> </ul>	
Controls Coverage Report	<p>Displays the percentage of controls for each authority document that are covered by at least one control test definition. Use this report to ensure that the appropriate controls are covered by the control test definitions to meet compliance goals.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Authoritative Source [grc_authoritative_source]</li> </ul>	<p>My GRC portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_admin</li> <li>grc_executive_approver</li> </ul> <p>My GRC Control</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_process_owner</li> <li>grc_test_definition_admin</li> </ul>	
Control Tests by Audit	<p>Lists all the control tests for an audit together with their state and short description. By default, the results are grouped by Audit and ordered by Control test and Audit number.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Control Test Status by Audit [grc_audit_control_test_view]</li> </ul>	<p>My GRC portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_admin</li> <li>grc_executive_approver</li> </ul>	<p>grc_audit_control_test_view</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Audit [grc_audit]</li> <li>Audit Control Test Instances [m2m_audit_control_test]</li> <li>Control Test Definition [grc_control_test]</li> </ul>



Report	Description	GRC portal	Database view
Control Tests by State (My Group)	<p>Displays control tests grouped by state for open audits that are owned by the logged-in user's group.</p> <ul style="list-style-type: none"> <li>Type: Pie chart</li> <li>Table: Control Test Status by Audit [grc_audit_control_test_view]</li> </ul>		<p>grc_audit_control_test_view</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Audit [grc_audit]</li> <li>Audit Control Test Instances [m2m_audit_control_test]</li> <li>Control Test Definition [grc_control_test]</li> </ul>
Failing Controls by Authority Document	<p>Displays failing control tests grouped by pertinent authority documents.</p> <ul style="list-style-type: none"> <li>Type: Pie chart</li> <li>Table: Control Authoritative Source [m2m_control_authoritative_source]</li> </ul>	<p>My GRC portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_admin</li> <li>grc_executive_approver</li> </ul>	
Manual Attestations Past Due Date	<p>Displays all overdue manual attestations for control tests attached to audits owned by the logged-in user.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: GRC Attestations by Control Test [grc_attestations_control_tests]</li> </ul>	<p>My GRC Audit portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_audit_definition_admin</li> <li>grc_internal_auditor</li> </ul>	<p>grc_attestations_control_tests</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Assessment Instance [asmt_assessment_instance]</li> <li>Control Test [grc_control_test]</li> </ul>
My Audits by State	<p>Displays the audits assigned to the logged-in user, grouped by state.</p> <ul style="list-style-type: none"> <li>Type: Pie chart</li> <li>Table: Audit [grc_audit]</li> </ul>	<p>My GRC Audit portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_audit_definition_admin</li> <li>grc_internal_auditor</li> </ul>	
My Audits in Progress	<p>Lists audits with a state of Work in Progress that are owned by the logged-in user.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Audit [grc_audit]</li> </ul>	<p>My GRC Audit portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_audit_definition_admin</li> <li>grc_internal_auditor</li> </ul>	

Report	Description	GRC portal	Database view
My Control Test Definitions	Lists control test definitions created by the logged-in user or generated from a control owned by the user or the user's group. <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Control Test Definition [grc_control_test_definition]</li> </ul>	My GRC Control portal Roles: <ul style="list-style-type: none"> <li>grc_test_definition_admin</li> <li>grc_process_owner</li> </ul>	
My Control Tests by State	Displays control tests grouped by state for open audits owned by the logged-in user. <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Control Test Status by Audit [grc_audit_control_test_view]</li> </ul>	My GRC Audit portal Roles: <ul style="list-style-type: none"> <li>grc_audit_def_admin</li> <li>grc_internal_auditor</li> </ul>	grc_audit_control_test_view Joins: <ul style="list-style-type: none"> <li>Audit [grc_audit]</li> <li>Audit Control Test Instances [m2m_audit_control_test]</li> <li>Control Test Definition [grc_control_test]</li> </ul>
My Controls by Authority Document	Displays controls owned by the logged-in user, grouped by authority document. <ul style="list-style-type: none"> <li>Type: Pie chart</li> <li>Table: Control Authoritative Source [m2m_control_authoritative_source]</li> </ul>	My GRC Control portal Roles: <ul style="list-style-type: none"> <li>grc_test_definition_admin</li> <li>grc_process_owner</li> </ul>	
My Failing Control Tests by Control	Displays a list of the logged on user's controls that are failing. Controls selected are active and pertinent. <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Control [grc_control]</li> </ul>	My GRC Audit portal Roles: <ul style="list-style-type: none"> <li>grc_test_definition_admin</li> <li>grc_internal_auditor</li> </ul>	grc_audit_control_test_view Joins: <ul style="list-style-type: none"> <li>Audit [grc_audit]</li> <li>Audit Control Test Instances [m2m_audit_control_test]</li> <li>Control Test Definition [grc_control_test]</li> </ul>

Report	Description	GRC portal	Database view
My Failing Controls by Authority Document	<p>Displays failing control tests generated from the logged-in user's control or control test definition, grouped by authority document.</p> <ul style="list-style-type: none"> <li>Type: Pie chart</li> <li>Table: Control Authoritative Source [m2m_control_authoritative_source]</li> </ul>	<p>My GRC Control portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_test_definition_admin</li> <li>grc_process_owner</li> </ul>	
My GRC Update Approvals	<p>Displays all GRC update activity for the logged-in user's approval group. This report does not show GRC update requests submitted when the Automatically approve all GRC update requests property is set to true. For additional information, see <a href="#">Approve a UCF document request - Legacy</a> on page 245.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: GRC Update Status [grc_ucf_update_status]</li> </ul>	<p>My GRC portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_admin</li> <li>grc_executive_approver</li> </ul>	
My Open Control Tests	<p>Lists open control tests for audits assigned to the logged-in user or user's group or audit definitions owned by the user or user's group.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Control Test Status by Audit [grc_audit_control_test_view]</li> </ul>	<p>My GRC Audit portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_audit_definition_admin</li> <li>grc_internal_auditor</li> </ul>	<p>grc_audit_control_test_view</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Audit [grc_audit]</li> <li>Audit Control Test Instances [m2m_audit_control_test]</li> <li>Control Test Definition [grc_control_test]</li> </ul>

Report	Description	GRC portal	Database view
My Observations and Remediations	<p>Lists observations and remediations for audits assigned to the logged-in user or user's group or audit definitions owned by the user or user's group.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Remediation by audit [grc_remediations_by_audit]</li> </ul>		<p>grc_remediations_by_audit</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Audit [grc_audit]</li> <li>Observation [grc_observation]</li> <li>Remediation [grc_remediation]</li> </ul>
Observations by Audit	<p>Lists all the observations for a given audit. By default, the results are grouped by Audit and ordered by Audit number and Observation.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Observation by Audit [grc_observations_by_audit]</li> </ul>		<p>grc_observations_by_audit</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Audit [grc_audit]</li> <li>Observation [grc_observation]</li> </ul>
Policy Coverage Gap	<p>Lists all policies linked to controls that are not used in any control test definition.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: GRC Policy Coverage Gap [grc_policy_coverage_gap]</li> </ul>		<p>grc_policy_coverage_gap</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Policy Control [m2m_control_policy]</li> <li>Control Test Definition [grc_control_test_definition]</li> </ul>
Remediations by Audit	<p>Lists remediations by audit. By default, the results are grouped by Audit number and Remediation. Remediations are generated when control tests fail.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Remediations by audit [grc_remediations_by_audit]</li> </ul>	<p>My GRC portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_admin</li> <li>grc_executive_approver</li> </ul>	<p>grc_remediations_by_audit</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Audit [grc_audit]</li> <li>Observation [grc_observation]</li> <li>Remediation [grc_remediation]</li> </ul>

Report	Description	GRC portal	Database view
Remediations by Observations	<p>Lists the remediations for each observation in an audit. By default, the results are grouped by Audit number. Remediations are generated when control tests fail.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Remediations by observation [grc_remediations_by_observations]</li> </ul>	<p>My GRC portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_admin</li> <li>grc_executive_approver</li> </ul>	<p>grc_remediations_by_observations</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Audit [grc_audit]</li> <li>Observation [grc_observation]</li> <li>Remediation [grc_remediation]</li> </ul>
Risk Coverage Gap	<p>Lists all risks linked to controls that are not used in any control test definition.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: GRC Risk Coverage Gap [grc_risk_coverage_gap]</li> </ul>		<p>grc_risk_coverage_gap</p> <p>Joins:</p> <ul style="list-style-type: none"> <li>Risk Control [m2m_risk_control]</li> <li>Control Test Definition [grc_control_test_definition]</li> </ul>
Super Control	<p>Lists the controls linked to more than one authority document and displays their compliance and non-compliance.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: Control [grc_control]</li> </ul>	<p>My GRC portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_admin</li> <li>grc_executive_approver</li> </ul> <p>My GRC Audit portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_audit_definition_admin</li> <li>grc_internal_auditor</li> </ul> <p>My GRC Control portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_test_definition_admin</li> <li>grc_process_owner</li> </ul>	

Report	Description	GRC portal	Database view
UCF Update Overview	<p>Lists the differences between the existing GRC entities and the available UCF updates. This report also displays the UCF release version and update time stamp. Results are grouped by the UCF authority document name. To see a result list longer than twenty entries, click the group title.</p> <ul style="list-style-type: none"> <li>Type: List report</li> <li>Table: GRC UCF Difference [grc_ucf_difference]</li> </ul>	<p>My GRC portal</p> <p>Roles:</p> <ul style="list-style-type: none"> <li>grc_admin</li> <li>grc_executive_approver</li> </ul>	

## GRC report interpretation - Legacy

Learn to interpret the reports for compliance, pertinence settings, and audit results.

### Compliance reports

A GRC user can report on the percentage of completion and percent compliant for all control test instances associated with an authority document, risk, and policy, to ensure that the company meets its compliance goals.

**Table 91: GRC compliance report definitions**

Report	Definition
Compliance	Percentage of control test instances that were successful for the last run.
Non-Compliance	Percentage of control test instances that failed for the last run.
Complete	Percentage of control test instances that either passed or failed for the last run.

### Pertinent and non-pertinent documents

Some controls that you import from UCF might not be relevant to your organization's compliance efforts. By default, compliance reporting excludes GRC components in which the Pertinent flag is set to false. Only controls in which this flag is set to true are rolled up in compliance reports to show their impact at the authority document level. Audit reports include all controls, regardless of the state of the Pertinent flag, to accurately represent the contents of the audit.

## Audit reports

Members of an internal or external audit team can use these reports to view an audit instance together with the results of the control tests. Open a specific control test instance containing the results to view audit details and the related observations and remediations.

## Customize a GRC report - Legacy

Users with the admin role can edit existing GRC reports or generate new ones.

1. Navigate to Reports View/Run .
2. Enter all or part of the report name in the Reports search field.

Users with the grc\_admin role can use the GRC reports as gauges in the My GRC portals.

## GRC risks, risk criteria, and risk approach rules - Legacy

A risk is a defined consequence that can occur if a policy is ignored. Risk criteria values are stored in the Risk Criteria [grc\_risk\_criteria] table. Approach rules are a short description of the approach philosophy that will be used to mitigate the risk. Demo data in GRC provides a default range of criteria levels from least to most for both types.

## Define a GRC risk - Legacy

Use the Risk form to define a new risk.

1. Navigate to GRC Risks .
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 92: Risk form fields**

Field	Description
Risk ID	A unique number assigned to the risk by the system.
Name	The name of the risk.
Significance	The impact of the risk if it is realized. Defined by risk criteria.
Likelihood	The probability that the risk will be realized. Defined by risk criteria.
Recommended approach	A reference to the risk approach rule Defining GRC Risks#Defining a Risk Approach Rule that determines how to treat this risk. Can be calculated dynamically using the Calculate Risk Approach UI action on the form.

Field	Description
Pertinent	Indicator that shows if a risk document is relevant to your organization. By default, this check box is selected and has a value of True. Clear this check box to mark this risk as not pertinent to your organization and to prevent it from appearing in compliance reporting.
State	A choice field for the state of the risk. Choose from: <ul style="list-style-type: none"> <li>• Known: The existence of the risk is known. This is the default value.</li> <li>• Open: The risk has been analyzed.</li> <li>• Issue: The risk has occurred.</li> <li>• Closed: The risk is no longer valid. For example, the risk was related to mainframes, but the organization no longer uses mainframes.</li> </ul>
Category	What category of risk applies to the record.
Compliance	[Read-only] Percentage of compliant control test instances associated with this risk.
Non-compliance	[Read-only] Percentage of non-compliant control test instances associated with this risk.
Applies to	A Document ID field to identify the scope.
Description	A verbose description of the risk.
Additional information	Information of any type that is pertinent to this risk.

4. Click Submit.

## Define GRC risk criteria - Legacy

Use the Risk Criteria form to define risk criteria.

In the base GRC system, the risk criteria available on the form are Significance and Likelihood.

1. Navigate to GRC Administration Risk Criteria .
2. Click New.
3. Fill in the fields on the form, as appropriate:

**Table 93: Risk criteria fields**

Field	Description
Type	Select one of the types provided, either Likelihood or Significance.



Field	Description
Display value	Create a name for the criteria that displays in the choice list. For example, enter 3 - Expected Behavior for the Likelihood type.
Order	The order in which this choice appears in the choice list. This order should be logical for the level selected.
Weighting	A numeric value for the risk, used to calculate risk approach rules. Low weighting factor indicates a lower overall risk, and high weighting factor indicates a higher overall risk.

4. Click Submit.
5. To select the new criteria in a risk record, navigate to **GRC Risks** and click **New**.
6. Open the choice list for the Likelihood field.

The new criteria appears in the list by its display name.

The screenshot shows a 'Risk' form with the following fields and values:

- Risk ID:** RISK0002002
- Name:** (Required field, marked with a red asterisk)
- Significance:** -- None --
- Likelihood:** -- None -- (Dropdown menu is open, showing options: -- None --, 5 - Extremely Likely, 4 - Improbable, 3 - Expected Behavior, 4 - Unexpected, 2 - Unknown, 1 - Unlikely)
- Recommended approach:** (Dropdown menu)
- Pertinent:** (Dropdown menu)
- Description:** (Text area)

## Define a GRC risk approach rule - Legacy

Define a new risk approach rule using the Risk Approach Rules form.

1. Navigate to GRC Administration Risk Approach Rules .
2. Click New.
3. Fill in the fields on the form, as appropriate.

< ☰ Risk Approach Rules - Detect and Monitor 

 ? ⚙ Update Delete ↑ ↓

Recommended approach

Active

Applies to Risk [grc\_risk]

Condition

All of these conditions must be met

Description

Field	Description
Recommended approach	A short description of the approach philosophy that will be used to mitigate the risk.
Active	If checked, the approach will be available for selection.
Condition	A condition builder which determines what risks this approach will be applied to if the Calculate Risk Approach button is clicked.

Field	Description
	<p><b>Note:</b> The first condition that is matched wins, so when creating new risk approach rules ensure that the conditions do not overlap with other risk approaches.</p>
Description	A full description of the risk approach.

## GRC authority documents and GRC citations - Legacy

An authority document defines the external standards, frameworks, or regulations that a process must use. These are stored as references, from which policies can be defined. Create your own authority documents or download and import the UCF authority documents. Citation records contain the provisions of the authority document, which can be interrelated.

### GRC authority documents

Authority documents are used to define policies, risks, controls, audits, and other processes ensuring adherence to the authoritative content. Each authority document is defined by a master record on the Authoritative Source [grc\_authoritative\_source] table, with a related list of records from the Authoritative Source Content [grc\_authoritative\_src\_content] table.

### GRC citations

Citation records contain the actual provisions of the authority document, which can be interrelated using configured relationships. In this way, the relationships between different sections of the authority documents can be mapped to better record how the authority document is meant to be implemented. The same relationship mechanism can be used to document relationships across authority documents. This is important because different sources address the same or similar controls and objectives.

You can create citations or import them from UCF authority documents and then create any necessary relationships between the citations. See [UCF authority document import process - Legacy](#) on page 235.

## Create a GRC authority document manually - Legacy

Create an authority document.

1. Navigate to GRC Authority Documents Authority Documents .
2. Click New.
3. Fill in the fields on the form, as appropriate.
4. Right-click in the header bar and select Save from the context menu.
5. In the Citations related list, click New.
6. Fill in the fields on the form, as appropriate.
7. Click Submit.

## Create a GRC citation - Legacy

A citation can be created manually.

1. Navigate to GRC > Authority Documents > Authority Documents .

2. Open an authority document that needs a citation.
3. In the Authority Documents related list, click New.
4. Fill in the fields on the form, as appropriate.

< **Citation - 164.402** 

Update
Delete
↑
↓

* Name	<input type="text" value="Contamination control"/>	Type	<input type="text" value="Control"/>
Reference	<input type="text" value="164.402"/>	Pertinent	<input checked="" type="checkbox"/>
Authority Document	<input type="text" value="-- None --"/>		
Guidance	<input style="width: 100%;" type="text" value="Provide all work areas with controls and procedures for preventing contamination."/>		
Additional Information	<input style="width: 100%; height: 30px;" type="text"/>		

Update
Delete

**Related Links**

[Add related to](#)

[Add related from](#)

[View relationships](#)

**Controls (2)**
Policies
Related to
Related from
Other Versions

Controls
New
Edit...
Go to

Control

◀◀
◀
1
▶
▶▶

Citation = 164.402 > Control Active = true

		Control	Connected by
<input type="checkbox"/>		<a href="#">Maintain ventilation system</a>	(empty)
<input type="checkbox"/>		<a href="#">Test contamination warning system</a>	(empty)

Actions on selected rows... 

◀◀
◀
1
▶
▶▶

Table 94: Citation form fields

Field	Description
Reference	Arbitrary reference number. In the GRC application, multiple citation records can have the same reference number.
Name	User-defined name that identifies this citation.
Type	Type of citation created. This is an optional field and is not used for any processing. You can use the value in this field in reports or to query for records of a specific type.
Authority document	Name of the parent authority document for this citation. When you create citations from the authority document form, the system completes this field automatically.
Pertinent	Indicates if this citation is relevant to your organization. By default, this check box is selected and has a value of True. Clear this check box to mark this citation as not pertinent to your organization and to prevent it from appearing in compliance reporting. Components marked as <i>not pertinent</i> are unavailable for the calculated links that enable results to rollup for any GRC hierarchy.
Version	[Read-only] Version number for previous versions of this citation. This value is a simple integer that is incremented by the system each time the citation is updated. This field is hidden when the current version of the record is displayed. You can view all available versions by selecting records from the Other Versions related list.
Guidance	Specific details for this citation, including areas of emphasis or concern. For earlier versions upgraded to Fuji, the contents of the "Key areas" field is displayed in this field.
Additional information	Information of any type that is pertinent to this citation.

5. Click Update.

## Add a relationship between GRC citations - Legacy

You can define relationships between citations from within the citation form.

1. Navigate to GRC > Authority Documents > Citations .
2. Open one of the citations in the relationship.

3. Select either the Add related to or Add related from related links.
4. Complete the form using the field from the table.

**Table 95: Adding relationships between citations**

Field	Input Value
To	The content that is the object of the relationship.
Relationship	The Relationship Type.
From	The content that is the subject of the relationship.

The display-only fields at the bottom will display the information from the other Citation record.



### Add relationship ✕

\* From  
12.6.1

\* Relationship  
Is section of::Includes section 🔍 ℹ️

\* To  
12.5.1 🔍 ℹ️

\* Name  
Change control procedures

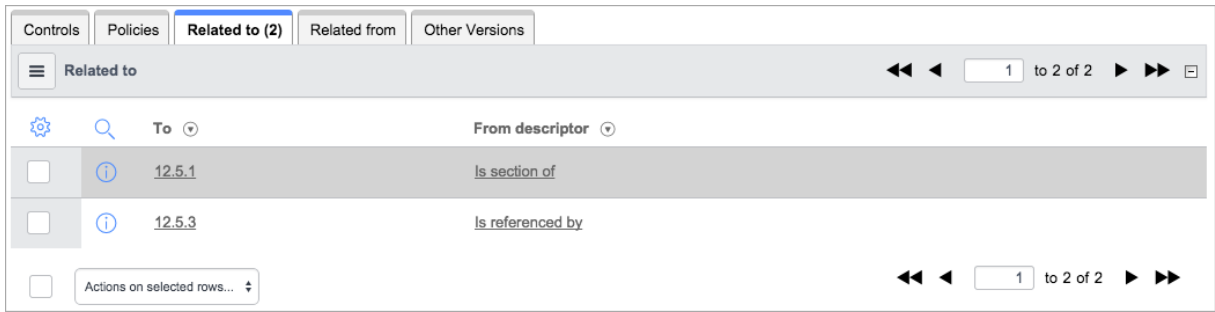
Authority Document  
ISO27002:2005 ⌵

Type  
Supporting Information ⌵

⌚

5. Click Submit.

The citation appears in the Related to or Related from related list, as appropriate.



### Define a GRC citation relationship type - Legacy

Relationships can be defined at the GRC citation level.

1. Navigate to GRC Authority Documents Relationship Type .
2. Click New.
3. Fill in the fields on the form, as appropriate.

**Table 96: Defining relationship types**

Field	Input Value
From descriptor	A description of how the relationship's subject relates to its object.
To descriptor	A description of how the relationship's object relates to its subject.
Name	A name for the relationship. Out-of-box relationship types use the format <from_descriptor>::<to_descriptor>
Active	If true, the relationship type will be available for selection.

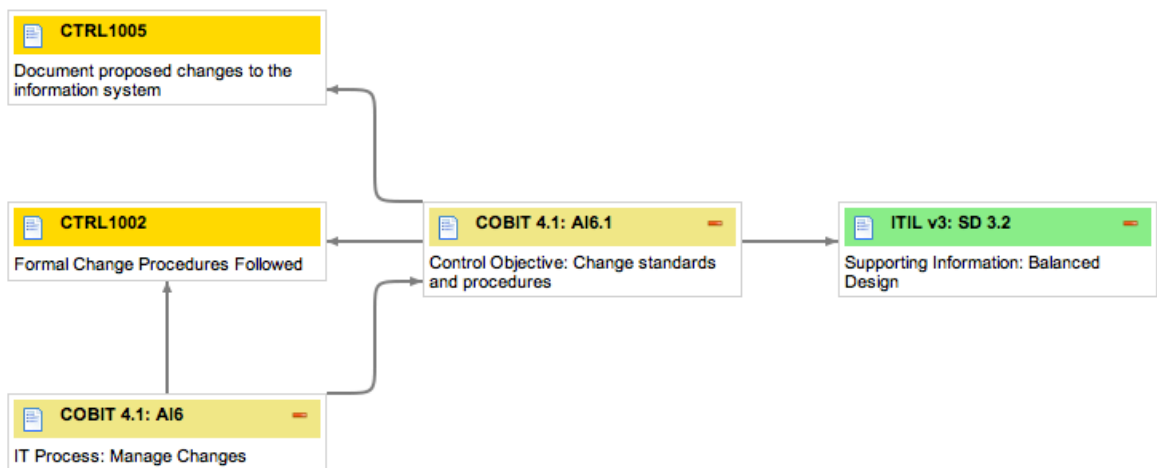
**Note:** Citations can also be associated with policies. For more information, see Managing Policies.

## View a relationship between GRC citations - Legacy

It is useful to view whether or not organizational controls are in place to address citations.

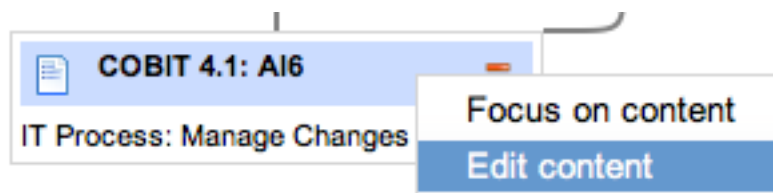
1. Navigate to GRC Authority Documents Citations .
2. Select a record.
3. Select the View Relationship related link.

This view is useful to visualize whether or not organizational controls are in place to address citations.



4. Click the + and - controls in the top right corner of the item to collapse or expand child items.
5. Right click any of the items to refocus the hierarchy on that item or to edit it.

The editing option opens the citation record.



When the items display, they appear in this format:

Authority Document: Citation

Citation Type: Short Description of Citation

## GRC policies - Legacy

A policy is a document which defines an internal practice that processes must follow. The Policy [grc\_policy] table extends Knowledge [kb\_knowledge], so each policy is stored in the Knowledge Base and can be accessed in the same way as any other published article.

### Standards and Standard Operating Procedures

GRC offers two additional policy classes called Standards and Standard Operating Procedures, that are used to define specific practices at different levels within an organization.

### Associations

To manage elements of the policy, the policy can be associated with:

- Scopes that define the level for which a policy class applies.
- Authority documents and citations to which a policy class applies.
- Risks associated with compliance failures.
- Controls that enforce the policy class and mitigate identified risks.

### GRC Policy enforcement

After policies are defined, there are two processes available for ensuring that their provisions are followed:

- Risk Managing: After risks are defined, they can be managed using Controls and Control Tests to protect against the consequences of breaching policies.
- Audits: After all the processes for policies have been defined, audits can be performed to confirm that they are being performed properly.

## Define a GRC policy, standard, or standard operating procedure - Legacy

The tables for standards and standard operating procedures extend the Policy [grc\_policy] table and provide the same information. The same procedure applies to defining a policy, a standard, or a standard operating procedures.

You can use standards and standard operating procedures to apply GRC policies to specific levels or scopes within an organization. For example, a scope can be an installation in another state that is subject to different regulations or a department that has to meet specific requirements.

1. Navigate to one of these locations:
  - GRC Policies
  - GRC Standards
  - GRC Standard Operating Procedures
2. Click New.
3. Fill in the fields on the form, as appropriate.

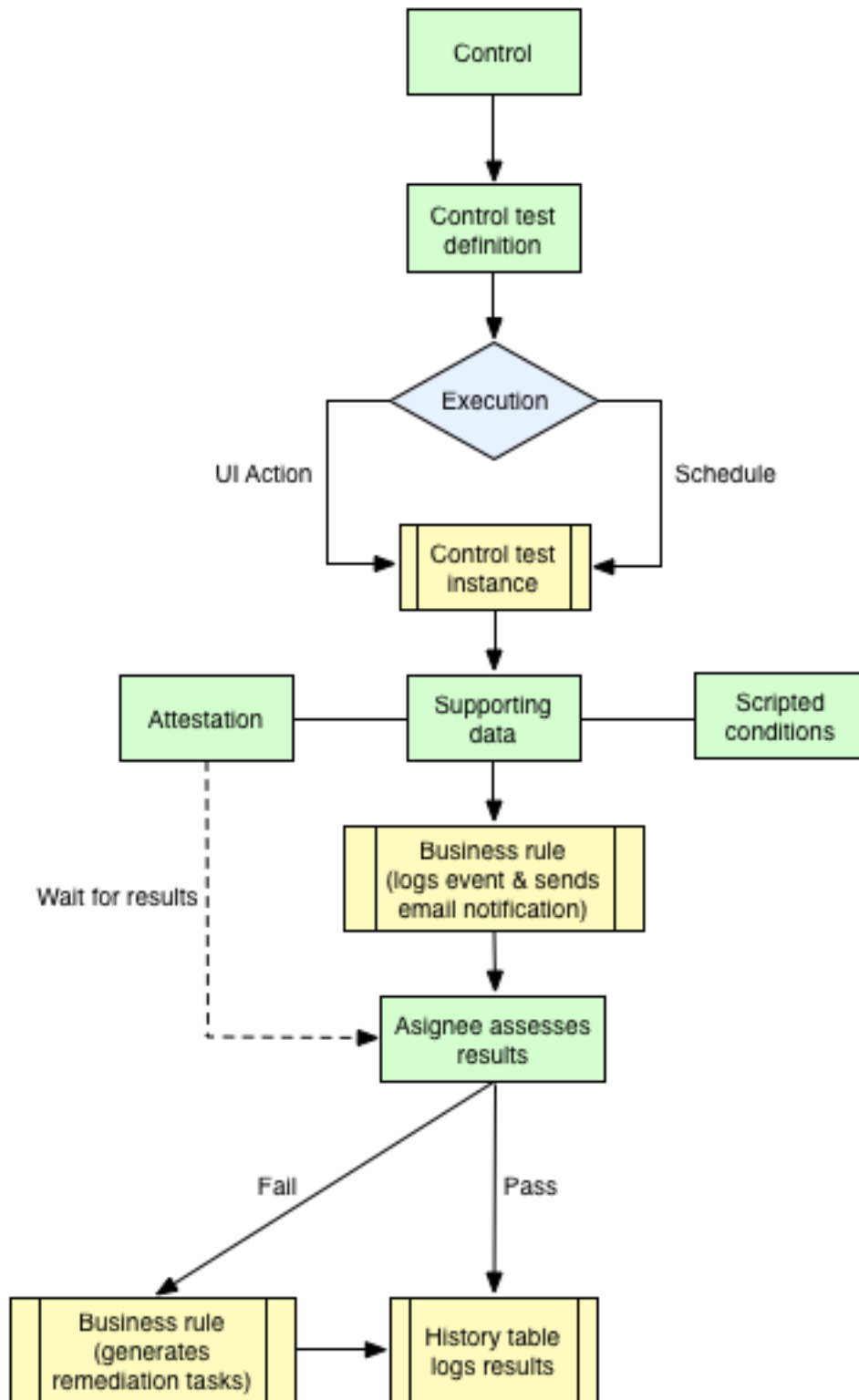
Field	Description
Number	A unique number assigned to the KB article using Number Maintenance.

Field	Description
Workflow	A stage field for how far along the policy is in the drafting process.
Article type	The type of markup used to write the article. Choices are HTML and Wiki.
Attachment link	Indicator that, if selected, opens the attachment rather than opening the policy in the Knowledge Base when the user selects the policy from the Knowledge Base.
Image	An icon to appear next to the policy in the Knowledge Base.
Pertinent	Indicator that determines if a policy is relevant to your organization. By default, this check box is selected. Clear this check box to mark this policy as not pertinent to your organization and to prevent it from appearing in compliance reporting.
Published	Date of publication.
Valid to	A date for the Policy to no longer appear in the knowledge base.
Parent policy	Reference field identifying a policy that is a parent to this policy. You can establish parent/child relationships between policies, standards, and standard operating procedures (SOP).
Compliance	[Read-only] Percentage of compliant control test instances associated with this policy.
Non compliance	[Read-only] Percentage of non-compliant control test instances associated with this policy.
Roles	The user roles required for users to see the article. If empty, everyone can see the policy. Once a role is input, only the selected roles can see the policy.
Short description	[Required] A unique description or title for this policy, standard, or SOP. The system displays this value for selection when you add link policies to a GRC entity record in the Policies related list. Make sure to provide a clear description that differentiates it from other policies, standards, or SOPs.
Text	The text of the policy, written in the appropriate markup language for the specified Article type.
Additional information	Information of any type that is pertinent to this policy.

## GRC controls and super controls - Legacy

After identifying risks, define controls or import them from UCF authority documents. A control is a process to mitigate risk, enforce a mandated policy statement, and address the directive of an authority document. The control may have one or many control tests associated with it. This ensures that the control is effective and provides continued compliance. Controls can also be directly associated with citations to map an organization's internal controls to those mandated by the authority document.

### Figure 7: GRC control process



### GRC super controls

A super control is a control shared by multiple authority documents.

When a new version of a super control is downloaded, the system links all authority documents using that control to the new version, even those authority documents not updated. This can result in unintended changes in the relationship between the shared control and any unmodified authority documents. Relationship changes can alter how compliance is evaluated for your organization. Be sure you know what affect these updated controls have on your audits.

The system displays super controls in:

- UCF document details
- GRC update requests
- GRC update approval records
- Email notifications

## Create a GRC control - Legacy

You can create GRC controls manually.

1. Navigate to GRC Controls All
2. Click New.
3. Fill in the fields on the form, as appropriate.



Control - Nightly security checks on manufacturing facilities.
Update Delete

Control ID: CTRL0002002

Owning group: Field Services

Owner: Keyna Bruni

Owner delegate: Genevieve Kekiwi

Pertinent:

Key control:

Name: Nightly security checks on manufacturing facilities.

Description: Evaluates effectiveness of nightly patrols by security guards in the manufacteiring facilities.

Additional information:

State: Active

Classification: Preventative

Purpose: Process

Control frequency: Continuous

Compliance: 0

Non compliance: 0

Update
Delete

Control Test Definitions (1)
Control Test Instances
Authority Documents
Citations
Policies
Risks
Other Versions

Control Test Definitions
New
Go to
Name
Search
1 to 1 of 1

Control = Nightly security checks on manufacturing facilities.
Run

<input type="checkbox"/>	ⓘ	Ensure that the facility is secure	▶	On Demand
--------------------------	---	------------------------------------	---	-----------

Actions on selected rows...
1 to 1 of 1

Table 97: Control form fields

Field	Description
Control ID	[Read-only] Unique identifier generated dynamically by the system.
Owning group	Group that owns the control.
Owner	User who owns the control.
Owner delegate	User who owns the control when the specified owner is unavailable.
Pertinent	Indicates that this control is relevant to your organization. By default, this check box is selected. Clear this check box if you do not plan to use this control and to prevent it from appearing in compliance reporting. Use this option to select appropriate controls from a large number of imported UCF controls.
Key control	Indicator that the control is considered key to preventing material risk, if selected.
State	Workflow field that determines the current state of the authoring process. Possible choices are: Draft, Active, and Inactive.
Classification	Control type being created. Possible choices are: Preventative, Corrective, and Detective.
Purpose	Approach that the control will take. Possible choices are: Process and Technical.
Control frequency	Basis for determining when the control is implemented. Possible choices are: Continuous, Event Driven, and Periodic.
Compliance	[Read-only] Percent of compliant control test instances associated with this control.
Non-compliance	[Read-only] Percent of non-compliant control test instances associated with this control.
Version	[Read-only] Version number for previous versions of this control. This value is a simple integer that is incremented by the system each time the control is updated. This field is hidden when the current version of the record is displayed. You can view all available versions by selecting records from the Other Versions related list.
Name	Descriptive name for this control.  -
Description	A verbose description of the control.

Field	Description
Additional information	Information of any type that is pertinent to this control.

You can configure the Control form to show these fields:

**Table 98: Additional fields for the Control form**

Field	Description
Authority document count	Total count of the authority documents that use this control. The purpose of this field is to calculate totals for the Super Control report.
Policy count	Total count of the policies that use this control. The purpose of this field is to calculate totals for the Super Control report.

## View a super control in a UCF document - Legacy

You can view super controls for all UCF documents you have downloaded and imported into GRC.

1. Navigate to [GRC Administration Import UCF Content](#).
2. Click a document card in the left column.

The system lists all shared controls for that authority document in the top portion of the details pane.

## 16 CFR Part 310 Details

Published name	16 CFR Part 310, Telemarketing Sales Rule (TSR)
Type	Regulation or Statute
Category	North America
Released version	Q4 14 - Final
Release date	2003-01-01
Effective date	2003-01-29
Impact zones	Privacy protection for information and data Records management
URL	<a href="#">16 CFR Part 310</a>

<u>GRC super controls</u>	<p>Related to: <a href="#">CobIT</a> by these controls:</p> <ul style="list-style-type: none"> <li>• <a href="#">Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.</a></li> </ul> <p>Related to: <a href="#">Australia CLERP</a> by these controls:</p> <ul style="list-style-type: none"> <li>• <a href="#">Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.</a></li> </ul> <p>Related to: <a href="#">10 CFR Part 73.54</a> by these controls:</p> <ul style="list-style-type: none"> <li>• <a href="#">Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.</a></li> </ul>
---------------------------	--

### View a super control in a GRC update request - Legacy

You can view super controls in the request form when updating UCF documents in GRC.

1. Navigate to GRC Administration Import UCF Content .
2. Import selected documents into GRC.

The request for approval screen indicates if the selected documents contain super controls.

### GRC Update Request for Approval ✕

12 CFR Part 229 (updates GRC Super Controls)  
16 CFR Part 310 Amendments

● Automatic approval is off, request will be sent for approval.

---

2 authority documents to request for approval.

## View a super control in a GRC update approval - Legacy

You can view super controls in the request form when updating UCF documents in GRC.

1. Navigate to Self Service My Approvals .
2. Select a UCF document update request.

The approval form shows the complete list of super controls for that document.

< **Approval** 

 ? 



↑ ↓

Approver

Approving

State

Comments

Created by admin

GRC Authority Documents [16 CFR Part 310](#)

UCF Authority Document [16 CFR Part 310](#)

Authority Document Source <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=bf60e7b87681ffc1030185f246d305&rgn=div5&view=text&node=16:1.0.1.3.34&idno=16>

GRC super controls Related to: [CobiT](#) by these controls:

- [Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.](#)

Related to: [12 CFR Part 229](#) by these controls:

- [Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.](#)

Related to: [10 CFR Part 73.54](#) by these controls:

- [Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.](#)

## View a super control in an email notification - Legacy

You can view super controls in email notification when authority documents are updated in GRC.

1. Navigate to [GRC Administration Import UCF Content](#) .
2. Update and authority document you currently use.

This action triggers an event called `control.versioned` which sends the Common control update email notification. By default, the system sends this notification to the GRC Executive Approver user and lists all super controls contained in the updated authority document.

## GRC control tests and definitions - Legacy

Control tests prevent issues from occurring. You can configure a control test definition to gather supporting data from any table using different condition types or through attestations sent to appropriate users. The control test definition determines how and when a control test is performed, including execution steps and expected results.

[Condition collections](#) can be created with associated conditions to define advanced control test logic. Each time the control test is performed, a control test instance is generated as a task to be executed, according to the control test definition.

[Certification filters](#) and [templates](#) simplify the selection of records to test. Certification filters provide the scope for test definitions by filtering a table for specific records. Attach the filter to a template that tests specific attributes of the filtered records.

The control test definition includes the ability to define the remediation group that is automatically assigned to a remediation task if the control test instance state is set to Failure.

## Modify the GRC control test definition - Legacy

Copy the existing control test definition provided by GRC and replace the condition collection with the certification filter and template you created in the previous procedures.

1. Navigate to [GRC Administration Control Test Definitions](#) .
2. Select the [All vendors have an NDA record](#).
3. Right-click the header bar and select [Insert and Stay](#) from the context menu.  
This action saves a copy of the control test definition record.
4. Change the name of this record to [All vendors have an NDA \(template\)](#) to differentiate it from the provided version.

This record uses a condition collection, specified in the [Configuration](#) field, called [All Vendors have an NDA](#).

**Control Test Definition** = Required field Update Execute Now Delete

Definition ID: CTD0001015 State: Active

Name: All vendors have an NDA Run: On Demand

Control: All vendors must have a Non-Disclosure agreement Control from demo data

Method: Assign to Individual

Assign to: Beth Anglin

Remediation group:

Execution step: [-]

Verify that all vendors have an active NDA

Expected result: [-]

No records should be returned - all vendors should have an NDA

Include supporting data:

Data purpose: Identifies non compliance

Table: Company [core\_company]

Fields: Name, Vendor

Condition type: Advanced

In scope definition: All Vendors Condition collection from demo data

Configuration to retrieve: Non Matching

Configuration: All Vendors have an NDA

Update Execute Now Delete

5. In the Condition type field, select Template.  
The system displays the Template field and hides the fields used for condition collections. The Configuration to retrieve is preset to Non Matching, which returns a list of vendors who do not have active non-disclosure agreements.
6. In the Template field, select the active version of Vendors with an NDA.



Control Test Definition ! = Required field

Update Execute Now Delete

Definition ID: CTD0002001 State: Active

Name: All vendors have an NDA (template) Run: On Demand

Control: All vendors must have a Non-Disclosure agreemen

Method: Assign to Individual

Assign to: Beth Anglin

Remediation group:

Execution step:

Verify that all vendors have an active NDA

Expected result:

No records should be returned - all vendors should have an NDA

Include supporting data:

Data purpose: Identifies non compliance

Table: Company [core\_company]

Fields: Name, Vendor

Condition type: Template

Configuration to retrieve: Non Matching

Template: Vendors with an NDA - 2

Update Execute Now Delete

#### 7. Click Update.

The system is configured for a GRC audit of vendors who do not have active contracts with non-disclosure agreements.

### Create a GRC certification filter - Legacy

ServiceNow does not include an NDA filter for vendors with GRC.

1. Navigate to GRC Administration Filters .
2. Click New.

3. Name the filter All vendors.
4. Select Company [core\_company] as the table.
5. Create a single condition that selects all vendors: [Vendor] [is] [true]  
This condition selects all records in the Company [core\_company] table that are marked as vendors.

6. Fill in rest of the form and click Submit.  
The system creates version 1 of this filter and marks it Active. A message in the Filter Condition field indicates that the condition contains 77 matching records.

## Create a GRC certification template - Legacy

After you create the filter that identifies the vendor records to audit, create a template that sets the audit conditions.

The system looks in the Contract [ast\_contract] table for all vendors that have the NDA contract model.

1. Navigate to GRC Administration Templates .
2. Click New.  
The Audit type field is read-only and is preset to Compliance. All templates created from within IT Governance Risk and Compliance use this audit type.
3. In the Name field, enter Vendors with an NDA.
4. Select the All vendors filter you created in the previous section.  
The condition builders appear. All conditions are [and] conditions.
5. In Certification Related List Conditions, create these conditions on the Contract [ast\_contract] table:
  - [Contract->Vendor] [State] [is] [Active]: Selects all vendors with an active contract.
  - [Contract->Vendor] [Contract model] [is] [NDA]: Selects all vendors with an NDA contract. For more information about completing the template form, see Creating Templates.

← Certification Template ! = Required field
Update Clone Delete

Number:  Active:

Name:

Description:

Filter:  Version:

Table:  Audit type:

**Certification Attribute Conditions**

	Condition
	<i>Insert a new row...</i>

**Certification Related List Conditions**

	Condition
✖	Contract->Vendor: "State" is "Active"
✖	Contract->Vendor: "Contract model" is "NDA"
	<i>Insert a new row...</i>

Update Clone Delete

**Related Links**  
[Delete unused versions](#)

6. Click Submit.

## GRC audits, audit observations and remediation tasks - Legacy

An audit definition establishes a set process for validating controls and control tests. From the definition, audit instances can be generated as a task to power the audit. During the audit process, audit observations can be recorded by the auditor to track the gathered information. The auditors can use these observations to create remediation tasks.

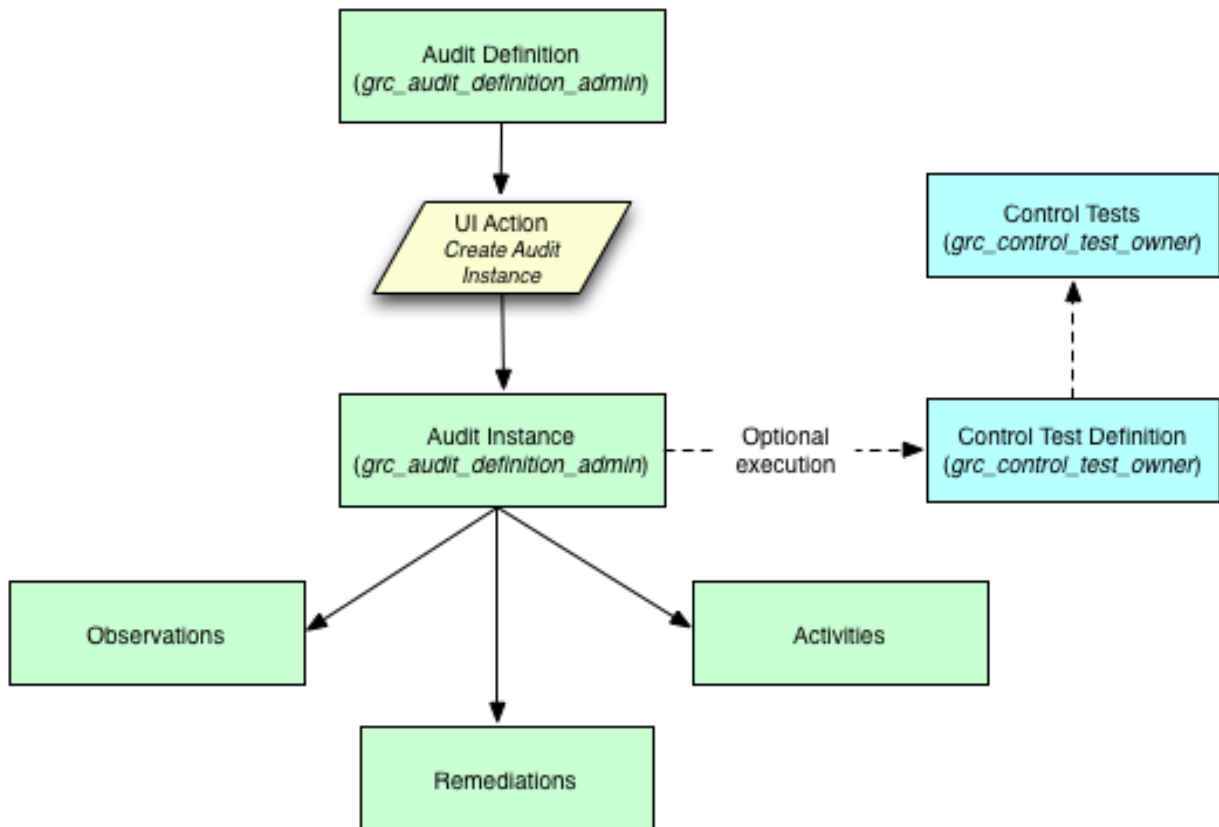
Once generated, audit instances can reference any existing evidence of compliance by associating previously executed control tests with the control test definitions that have been established in the audit.

During the audit process, an administrator can create and assign remediation tasks that need to be performed before and during an audit. In addition, audit requirements associate citations to the audit, allowing auditors to track compliance or non-compliance with the original regulations.

If the latest evidence is not recent enough, click Execute Now in the Control Test Definition form to execute a control test instance. This action creates the control test instance and automatically associates it to the audit. The control test instance record also has the Generate from audit field populated with the audit number, so that it is clear that the test was created from an audit and not manually.

The following diagram illustrates the process of managing an audit with IT Governance, Risk and Compliance:

**Figure 8: GRC audit process**



## Define a GRC audit requirement - Legacy

Audit Requirements can be defined to create a relationship between the audit and authoritative source content, allowing auditors to determine whether the audit is in compliance with particular sections of regulation or policy.

1. Navigate to GRC Audit Definitions .
2. Click Edit in the Requirements related list and add authoritative source content.
3. After you add the audit requirements to the list, click Edit in the Control Test Definitions related list and add a definition to associate with the control test.

After the audit requirements are associated with the audit definition, these requirements create Requirements records associated to each audit instance generated. The Requirements form has the following fields:

Table 99: Audit Requirements

Field	Input Value
Number	A number identifier for the requirement.
Requirement	A reference to the Authoritative Source Content which contains the original source of this requirement.
Name	The name field from the Authoritative Source Content record.
Type	The type field from the Authoritative Source Content record.
Authoritative Source	The authoritative source field from the Authoritative Source Content record.
Control test definition	The control test associated with the requirement.
Supporting control test	The control test instance whose results are either compliant or not compliant with this requirement.
Compliant	A check box to record whether the audited subject is compliant with this requirement.
State	The state field from task.
Assignment group	A group assigned to assess the requirements.
Assigned to	A user assigned to assess the requirements.

## Create a GRC audit definition - Legacy

An audit definition establishes a set process for validating controls and control tests. From the definition, audit instances can be generated as a task to power the audit.

1. Navigate to GRC Administration Audit Definitions .
2. Click New.
3. Fill in the fields on the form, as appropriate.

Field	Input Value
ID	A unique ID for the audit definition, populated by Number Maintenance.
Name	A name for the audit definition.
Owning group	A reference to a group to have ownership over the audit process.
Owner	A reference to a user to have ownership over the audit process.
Execution group	A reference to the group that will execute the audit.

Field	Input Value
Type	The type of audit process.
State	Where in the drafting process the definition is.
Short description	A short description of the audit.
Description	A full description of the audit.

4. Use the related list Control Test Definitions to specify control tests to perform during the audit.
5. Use the related list Scope to define entities for the audit to refer to.

## Run the GRC vendor audit - Legacy

After creating the audit definition, you are ready to run the audit.

1. Navigate to GRC Administration Control Test Definitions .
2. Select the All vendors have an NDA (template) record.
3. Click Execute Now.  
The Control Test Definitions list appears.
4. Reopen the same record.
5. In the Control Test Instances related list, open the test instance you just created.
6. Scroll down to the Supporting Data section.

Name	Vendor
Acer	true
Adobe Systems	true
Adtran	true
Altiris	true
Amazon	true
America Online	true

The in scope records for this audit of the Company [core\_company] table were the 78 companies in the demo data defined as vendors. Of these 78, the audit returned 77 that did not match the template conditions.

Three of these 77 vendors did have an NDA contract, but the contracts were inactive, making them non-matching. ServiceNow matched the template conditions with only one active NDA contract that was not retrieved in the audit. Had you selected Matching in the Configuration to retrieve field of the control test definition, the support data would have shown only one matching vendor.

Contracts New Go to Number:  Q 1 to 4 of 4

Contract model = NDA

Number	Contract type	State	Substate	Vendor	Starts	Ends	Short description	Expiration level
CNTR0009043	Contract	Active		ServiceNow	2013-06-21	2013-07-20	Non-Disclosure agreement with ServiceNow	Within 30 days
CNTR0009044	Contract	Cancelled	Rejected	IBM	2012-10-20	2013-10-20	Non-Disclosure agreement with IBM as a v...	
CNTR0009045	Contract	Expired	Approved	Amazon	2011-10-21	2012-10-19	Non-Disclosure agreement with Amazon as ...	Expired
CNTR0009046	Contract	Draft	Approved	SpyBot	2013-10-21	2014-10-20	Non-Disclosure agreement with SpyBot as ...	

Actions on selected rows... 1 to 4 of 4

## Create a GRC audit instance - Legacy

An audit instance manages the audit process.

When the audit is defined and in the Current state, click Create Audit Instance under Related Links to generate an Audit Instance record.

The audit is automatically assigned to the owning group, and the event `grc_audit.inserted` is recorded in the event log by the business rule planned task global events. By default, any active control test definitions associated with the audit definition are executed and create control test instances when the audit instance is created.

< **Audit Definition - Building access security** 

Update Delete ↑ ↓

ID	<input type="text" value="AUD0002001"/>	State	<input type="text" value="Current"/>
Name	<input type="text" value="Building access security"/>	Execution group	<input type="text" value=""/>
Owning group	<input type="text" value=""/>	Owner	<input type="text" value="Alfonso Griglen"/>
Short description	<input type="text" value="Building access security practices"/>		
Description	<input type="text" value="Determine if proper procedures are being followed by security personnel during building access checks."/>		

Update Delete

**Related Links**

[Create Audit Instance](#)

Control Test Definitions New Edit... Go to

1 to 1 of 1

**Audit definition = Building access security**

	Control test definition	Control	State
<input type="checkbox"/>	<u>Ensure all entrances to buildings in San Deigo are pass card enabled</u>	All buildings fitted with electronic sec...	Active

Actions on selected rows...

1 to 1 of 1

Click to execute the control test definition





## Record GRC audit activities - Legacy

Audit Activities are used to record and track the tasks required to perform an audit instance.

1. To create an Audit Activity, navigate to the appropriate [audit instance](#).
2. In the Audit Activities related list, click New.
3. Populate the fields from the table.

**Table 100: Recording Audit Observations**

Field	Description
Number	An incremented identifier for the audit activity, generated by the system.
Requested By	A reference to the user who requested the audit activity.
Requestor Reference	A reference to a record in a third party system where the requestor may be tracking the requirement
Opened By	A reference to the user who created the audit activity.
Opened	A date-time stamp for when the audit activity was created.
State	A choice list for status of the task: <ul style="list-style-type: none"> <li>• Pending</li> <li>• Open</li> <li>• Work in Progress</li> <li>• Closed Complete</li> <li>• Closed Incomplete</li> <li>• Closed Skipped</li> </ul>
Assignment Group	A reference to the group assigned to perform the audit activity.
Assigned To	A reference to the user assigned to perform the audit activity.
Closed	A date-time stamp for when the audit activity was closed.
Closed by	A reference to the user who closed the record.
Short Description	A short description of the audit activity.
Description	A more detailed description of the audit activity.
Work Notes	A journal field for recording work performed on the audit activity.

## Record GRC audit observations - Legacy

The Audit Observations related list on the Audit record can be used to record any information uncovered in the audit process.

Remediation tasks can be generated directly from audit observations. For instance, the audit observation There is no process around off-boarding can lead to the remediation task Define off-boarding process.

Using the Related Items tool, audit observations can be related to any task on the platform by explicitly defined relationships.

1. Navigate to GRC Audit .
2. Select the appropriate audit instance.
3. In the Audit Activities related list, click New.
4. Relate audit observations to any task on the platform by explicitly defined relationships.
5. Fill in the fields on the form, as appropriate.

**Table 101: Recording Audit Observations**

Field	Input Value
Number	An incremented identifier for the audit activity.
Requested By	A reference to the user who requested the audit activity.
Requestor Reference	A reference to a record in a third party system where the requester may be tracking the requirement
Opened By	A reference to the user who created the audit activity.
Opened	A date-time stamp for when the audit activity was created.
State	A choice list for status of the task: <ul style="list-style-type: none"> <li>• Pending</li> <li>• Open</li> <li>• Work in Progress</li> <li>• Closed Complete</li> <li>• Closed Incomplete</li> <li>• Closed Skipped</li> </ul>
Assignment Group	A reference to the group assigned to perform the audit activity.
Assigned To	A reference to the user assigned to perform the audit activity.
Closed	A date-time stamp for when the audit activity was closed.
Closed by	A reference to the user who closed the record.
Short Description	A short description of the audit activity.

Field	Input Value
Description	A more detailed description of the audit activity.
Work Notes	A journal field for recording work performed on the audit activity.

## UCF authority document import process - Legacy

The GRC application downloads Unified Compliance Framework (UCF) authority documents and transforms selected data into the GRC application tables through an approval process. Administrators can filter the downloaded content, select the documents to use, and import only the content they want into tables for authority documents, citations, and controls. When UCF publishes quarterly updates, GRC determines which data in your system needs to be updated and displays side-by-side comparisons of the changes to make the process easier.

---

**Note:** For more information on Unified Compliance Framework (UCF), see <https://www.unifiedcompliance.com/>.

---

- Download the UCF documents, using the controls in the UCF Authority Documents screen.
- Select the documents you want to use for your authority documents, citations, and controls and request an import into GRC.
- Approve the request to import the content into the GRC tables.



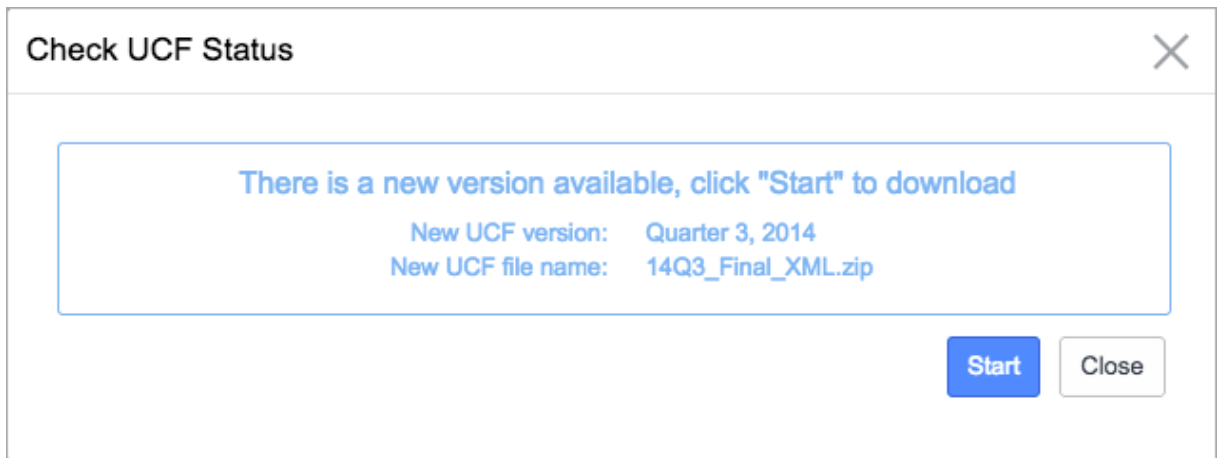
**Warning:** All data imported from UCF Authority Documents is read-only and must be protected. Do not customize the controls on any UCF fields transformed into GRC tables.

---

## Download a UCF file - Legacy

The UCF import process begins with downloading UCF documents.

1. Navigate to GRC > Administration > Import UCF Content , to open an empty UCF Authority Documents window.
2. Click Check UCF Status to open the Check UCF Status screen.



3. Click Start.

The status window shows the name and version of the file and the progress of the download. For more information, see [UCF Download Background Processes](#).

---

**Note:** If the internet connection is lost for any reason, a message appears in the bottom of the download screen advising you of this exception. The system attempts to reconnect to the UCF download site, and removes the message when communication is restored.

---

### Check UCF Status ✕

Status	Running
Current UCF version	Quarter 3, 2013
Current UCF file name	13Q3_Final_XML.zip
Started by	System Administrator
Time started	Tue Dec 30 12:48:25 PST 2014
Time finished	

Connect to server	✔	Connected successfully
Download Authority Documents	✔	Records downloaded: 596
Download Citations	✔	Records downloaded: 67770
Download Controls	✔	Records downloaded: 6759
Compare against GRC	✔	Up to date: 1; Update available: 1; Not imported: 594
Build filter table	☾	

**Build filter table** Run in background

4. When the download has completed successfully, click Done to view the UCF authority documents.

**Check UCF Status**
✕

Status	Finished
Current UCF version	Quarter 3, 2013
Current UCF file name	13Q3_Final_XML.zip
Started by	System Administrator
Time started	Tue Dec 30 12:48:25 PST 2014
Time finished	Tue Dec 30 12:53:52 PST 2014

Connect to server	✔	Connected successfully
Download Authority Documents	✔	Records downloaded: 596
Download Citations	✔	Records downloaded: 67770
Download Controls	✔	Records downloaded: 6759
Compare against GRC	✔	Up to date: 1; Update available: 1; Not imported: 594
Build filter table	✔	Table built successfully

Downloaded successfully
Done

## Select UCF content to import - Legacy

Select documents from the UCF download that you want to import into the GRC tables.

Your import selections go through an approval process before the system moves the documents into GRC tables.

1. Navigate to **GRC > Administration > Import UCF Content** .

The UCF Authority Documents screen appears, showing all the downloaded documents as *cards* in the left column.

2. To view the details of a document, click anywhere in the card.

The selected card is outlined in blue. A document counter at the top of the left column indicates the number of document cards displayed and also functions as a reset button for the filter and search box. The citations and controls associated with the selected document card appear in the detail pane

on the right. The current version of the UCF document appears in the Released Version field and is expressed as Qx YY - Final, where Q is the current quarter, and YY is the current year.

UCF Authority Documents 596

Search... Check UCF Status Update GRC

10 CFR Part 73.54

Version  
Last modified 2013-07-18  
Originator North American Electric Reliability Corporation  
GRC import status Not imported

12 CFR Part 205

Version  
Last modified 2013-07-18  
Originator US Congress  
GRC import status Not imported

12 CFR Part 229

Version  
Last modified 2013-07-18  
Originator US Congress  
GRC import status Not imported

12 CFR Part 748

Version July 1, 2001  
Last modified 2013-07-18  
Originator National Credit Union Association  
GRC import status Not imported

### 10 CFR Part 73.54 Details

Published name 10 CFR Part 73.54, Protection of digital computer and communication systems and networks

Type Regulation or Statute

Category Energy Guidance

Released version Q3 13 - Final

Release date 2009-10-30

Effective date 2009-11-23

Impact zones  
Human Resources management  
Operational management  
Records management  
Audits and risk management  
Technical security  
Physical and environmental protection

URL [10 CFR Part 73.54](#)

GRC super controls Related to: [HIPAA](#) by these controls:

- Establish and maintain a set of key policies, standards, and procedures to support confidentiality, integrity, availability, and accountability.

Related to: [CobIT](#) by these controls:

- Establish and maintain the IT governance risk assessment framework.
- Assign ownership of the organization's policies, standards, and procedures to the appropriate organizational role.
- Communicate security awareness and the internal control framework to all constituents.
- Retain records in accordance with applicable regulations.
- Establish and maintain a data retention policy and data retention processes and determine how long to to keep records and logs.
- Detect and react to inappropriate usage red flags and inappropriate usage incidents in a timely basis.
- Monitor systems for inappropriate usage and other security violations.
- Technical security

Document display counter and filter reset control

Details pane



3. Type a string in the search box to filter the cards by values in the documents' headers.

You can search on these UCF fields from the Details pane:

- GRC import status
- Category
- Type
- Originator
- Impact Zones

For example, a string search for us federal trade displays a document that contains US Federal Trade Commission in the Originator field.

The screenshot shows the 'UCF Authority Documents' interface. At the top, there is a search bar containing the text 'ftc'. Below the search bar, a list of documents is displayed, with one document selected: '16 CFR Part 310 Amendments'. The details pane for this document is open, showing the following information:

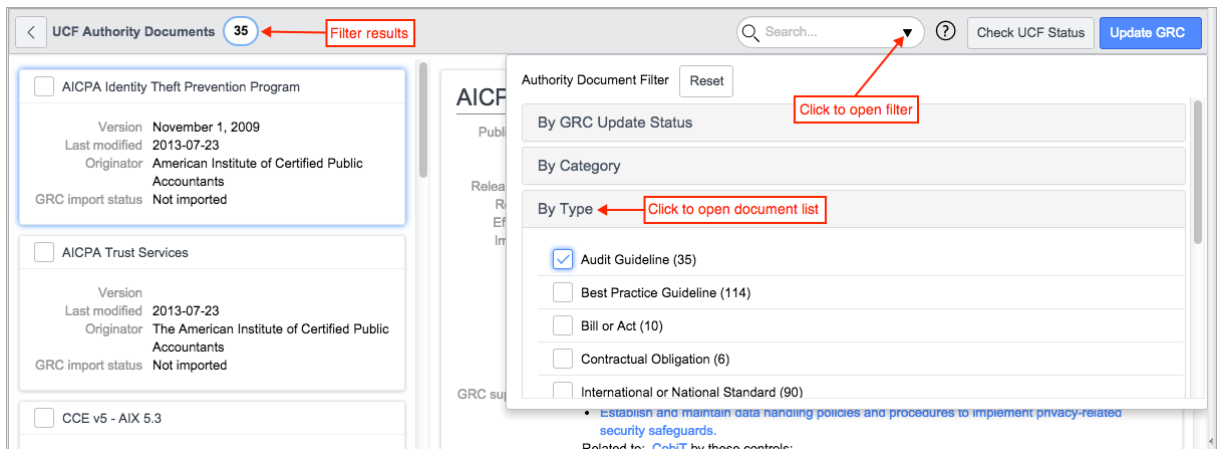
Version	
Last modified	2013-07-18
Originator	US Federal Trade Commission (FTC)
GRC import status	Not imported

The details pane also shows the following information:

Published name	16 CFR Part 310, Amendments to the FTC Telemarket
Type	Regulation or Statute
Category	US Federal Privacy Guidance
Released version	Q3 13 - Final
Release date	2003-01-01

A red arrow points from the search bar to the 'Originator' field in the details pane, which contains the text 'US Federal Trade Commission (FTC)'.

4. To clear the search field, click the counter at the top of the left column.
5. Click the arrow in the search field to display the authority document filter.



6. In the filter that appears, click a group heading to expand the section.

Each group is a field from the document header. The numbers in parentheses show the count of UCF documents in each group.

7. To filter the list by document status, select an option from the GRC Update Status section.

This list displays these document states:

- Up to date: Documents you have imported that are currently up to date in your system.
- Not imported: Available documents that you have not imported yet.
- Update available: Documents you have imported for which updates are available.

8. To filter the list by documents in similar categories, click a value in one or more of the groups provided.

9. Click one or more field values to filter the list and display the matching document cards in the left column.

The system applies the following operators to multiple filters:

- Filters within the same group or between groups have an OR relationship.

- Filters in the authority document filter have an AND relationship with a string in the search box.
10. Click Reset to clear the selections in the authority document filter, or click the counter above the left column.
  11. Select the check boxes in the cards for the documents you want to import into GRC.  
A counter on the Update GRC button shows the number of cards currently selected.

The screenshot displays the 'UCF Authority Documents' interface. On the left, there is a list of documents with checkboxes. The first document, 'Australia Spam Act of 2003', is selected. The right pane shows the details for this document, including its published name, type, category, release date, and impact zones. A red box highlights the 'Update GRC (5)' button in the top right corner, with an arrow pointing to it from a text box that says 'Count of documents selected for import'.

12. Click Update GRC.

The system displays an import dialog box that lists the requested documents and advises you if approvals are required for this request. The dialog box indicates if a selected document contains *super controls*. A super control is any control shared by two or more authority documents. When you import a document with super controls, GRC updates those controls for all authority documents that use them.

### GRC Update Request for Approval ✕

10 CFR Part 73.54 (updates GRC Super Controls)  
12 CFR Part 748 (updates GRC Super Controls) ← **Shared controls**  
16 CFR Part 310 (updates GRC Super Controls)  
Australia Spam Act of 2003  
Australian Government Information Security Manual Controls (updates GRC Super Controls)

● Automatic approval is off, request will be sent for approval.

---

5 authority documents to request for approval. Submit Close

13. Click Submit to initiate the approval process.

When the request is submitted, the dialog box lists the approval status of each document you have selected. If a document was previously requested but has not yet been approved, GRC marks it Awaiting approval.

14. Click Close.

### GRC Update Request for Approval ✕

✓ 10 CFR Part 73.54 (updates GRC Super Controls)	Requested
✓ 12 CFR Part 748 (updates GRC Super Controls)	Requested
✓ 16 CFR Part 310 (updates GRC Super Controls)	Requested
✓ Australia Spam Act of 2003	Requested
✓ Australian Government Information Security Manual Controls (updates GRC Super Controls)	Requested

● Automatic approval is off, request will be sent for approval.

---

Request submitted, once approved, they will be updated automatically. Close

## Approve a UCF document request - Legacy

By default, UCF authority documents selected for import or update require approval before GRC can move the data into the appropriate tables.

When an administrator submits a UCF document request, the system sends email notifications to all members of the GRC Approvers group and creates an approval task. Only one member of the group is required to approve or reject a UCF request. The GRC Approvers group contains members with the `grc_admin` or `grc_executive_approver` role.

When a request is approved, the system updates GRC appropriately. Depending on the size of the UCF document, this process can take several minutes. The system notifies the requester by email when the update is complete, and the data is ready for use. If the update request is rejected, the system sends the notification immediately.

A system property determines whether or not an approval is required for UCF imports. Navigate to `GRC > Administration > Properties` and locate the property named `Automatically approve all GRC update requests`. By default, this property is set to require approvals. To make approvals automatic for all requested UCF imports, select the Yes check box.

---

**Note:** The download process overwrites all UCF documents in the staging tables, including those awaiting approval. For this reason, the system prevents you from downloading new versions of UCF authority documents either manually or automatically if you have pending approval requests

for GRC updates. To proceed, you must approve or reject all pending requests before the system can download new authority documents.

1. Navigate to **Self-Service > My Approvals**.

The list contains approval requests in any state that are assigned to your group.

2. To approve or reject multiple requests, you can edit the State column in the list.

State	Approving	Approver	Comments	Approval for	Created
Not Yet Requested		System Administrator			2014-12-30 15:20:55
Requested		System Administrator			2014-12-30 15:20:56
Approved		System Administrator			2014-12-30 15:20:56
Rejected		System Administrator			2014-12-30 15:20:56
Cancelled		System Administrator			2014-12-30 15:20:56
No Longer Required		System Administrator			2014-12-30 15:20:56
More Information Required		System Administrator			2014-12-30 15:20:56
Duplicate		System Administrator			2014-12-30 15:20:56
Requested		System Administrator			2014-12-30 15:20:56
Requested		System Administrator			2014-12-30 15:20:56

3. To process a single UCF update requests, open the record and review the details.

< **Approval**

Approver

State

Comments

Created by **admin**

GRC Authority Documents [16 CFR Part 310](#)

UCF Authority Document [16 CFR Part 310](#)

Authority Document Source <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=bf60e7b87681fcbf1030185f246d305&rgn=div5&view=text&node=16:1.0.1.3.34&idno=16>

GRC super controls **Related to: [CobIT](#) by these controls:**

- [Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.](#)

**Related to: [10 CFR Part 73.54](#) by these controls:**

- [Establish and maintain a data retention policy and data retention processes and determine how long to keep records and logs.](#)

Approving

Activity  2014-12-30 15:20:56 **System Administrator** Changed: Approver, State

**Approver:** System Administrator

**State:** Requested

#### 4. Click Approve or Reject.

When you approve a request, the approval workflow sends an email to the requester describing the action taken on the request. By default, all approved UCF control documents are imported into GRC in an active state, ready for use. Depending on the size of the documents selected, the import process can take several minutes. The system moves the selected data from the UCF tables to the appropriate GRC tables as shown here.

**Table 102: Table mapping**

UCF Table	GRC Table
UCF Authority Document [ucf_authority_document]	Authoritative Source [grc_authoritative_source]
UCF Citation Mapping [ucf_citation_mapping]	Authoritative Source Content [grc_authoritative_src_content]
UCF Control [ucf_control]	Control [grc_control]

### UCF authority document update process - Legacy

You can update the UCF documents you use in GRC manually or configure the system to do it automatically whenever a new UCF version is available.

By default, GRC downloads the most recent version of the UCF authority documents, which are updated quarterly. The ServiceNow system places these files in staging tables until they are imported into GRC. When you import a new document version, these entities are updated:

- Authority documents
- Citations
- Controls

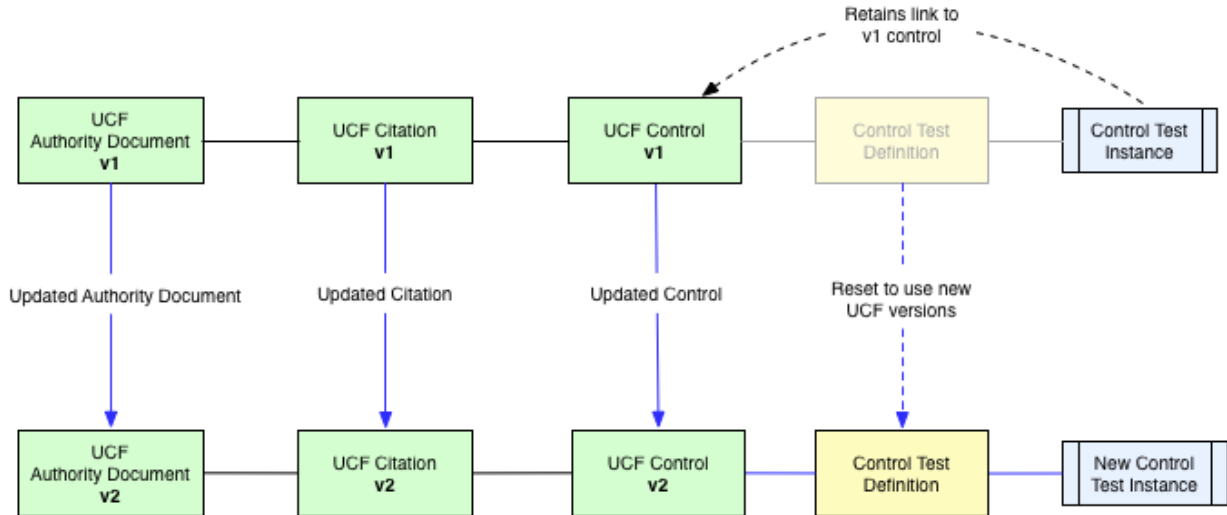
GRC observes these general rules when importing updated documents from UCF:

- If UCF authority documents or citations are updated, both entities are imported into GRC and versioned.
- If only the UCF controls are updated, then only the controls are versioned. In this case, a new link is created between the updated control and the existing citation that uses it.
- Older versions of updated controls are automatically deactivated and do not appear in lists of controls.

The control test definitions, policies, and risks that use these updated entities are reset to use the latest version. Any control test instances tied to a control from the previous version remain linked to that control. You must generate new control test instances based on the latest UCF version. The system deactivates all previous versions of an imported UCF document and retains them in their respective GRC tables.

#### Figure 9: Automatic updates to UCF links





Changes to these UCF authority document fields trigger versioning in GRC.

**Table 103: Authority document fields**

UCF Field	GRC Field
ucf_ad_common_name	name
ucf_ad_id	source_id
ucf_ad_version	source_version
ucf_ad_date_modified	source_last_modified
ucf_ad_release_version	source_release_version
ucf_ad_url	url

**Table 104: Citation fields**

UCF Fields	GRC Fields
ucf_citation	reference
ucf_citation_guidance	key_areas
ucf_citation_id	source_id
ucf_citation_date_modified	source_last_modified
ucf_citation_release_version	source_release_version

Table 105: Control fields

UCF Fields	GRC Fields
ucf_ce_control_title	name
ucf_ce_control_statement	description
ucf_ce_id	source_id
ucf_ce_date_modified	source_last_modified
ucf_ce_release_version	source_release_version

#### *Update a UCF document manually - Legacy*

By default, GRC is configured to require manual update of the UCF documents it uses.

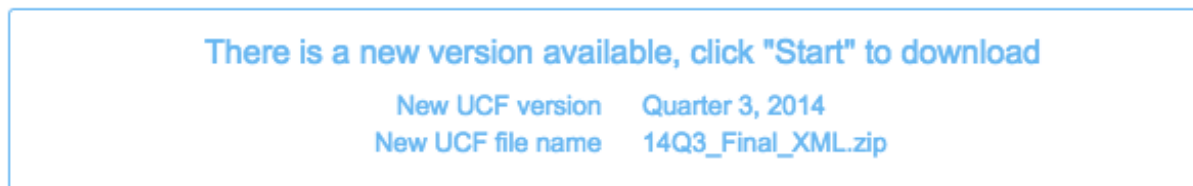
Resolve any pending approval requests for GRC updates before attempting to download new UCF documents. The system blocks the download until all requests are either approved or rejected.

1. Navigate to GRC > Administration > Import UCF Content

The UCF Authority Documents screen displays the current documents.

2. Click Check UCF Status.

The download screen appears, showing the results of the previous download, including the UCF file name. The system checks the UCF document version and displays a banner in the download screen advising if your version is current or can be updated.



3. To download a new version, click Start.

If you have pending approval requests for GRC updates, the system blocks the download.

4. Resolve any pending requests before proceeding

The download screen tracks the progress of the update. GRC downloads the latest UCF archive and unpacks it. The system then deletes the contents of the staging tables and reloads them with the latest data. There is no versioning used in these tables. During this operation, the system compares the incoming data with the current data in GRC to determine if anything has changed. When the update is finished, the download screen shows the results of the comparison.

---

**Note:** If the internet connection is lost for any reason, a message appears in the bottom of the download screen advising you of this exception. The system attempts to reconnect to the UCF download site and removes the message when communication is restored.

---

### Check UCF Status ✕

<b>Status</b>	Finished
Current UCF version	Quarter 3, 2014
Current UCF file name	14Q3_Final_XML.zip
Started by	System Administrator
Time started	Tue Dec 30 15:57:33 PST 2014
Time finished	Tue Dec 30 16:13:13 PST 2014

Connect to server	✔ Connected successfully
Download Authority Documents	✔ Records downloaded: 673
Download Citations	✔ Records downloaded: 98693
Download Controls	✔ Records downloaded: 9559
Compare against GRC	✔ Up to date: 4; Update available: 4; Not imported: 665
Build filter table	✔ Table built successfully

**Downloaded successfully** Done

5. Look at the value in the GRC Import Status field in the cards for the documents you use to see if updates are available.

Possible status values are:

- Up to date: Documents you have imported that are currently up to date in your system. There is no update available from UCF in the latest version. The check box for up to date items is disabled.
  - Not updated: Available documents that you have not imported into GRC.
  - Update available: Documents you have imported previously for which updates are available.
6. If the system indicates that an update is available, click the arrows on the card to view the difference between your current GRC data and the latest UCF version of that data.



A window appears, showing specific differences between the two versions. These conditions can occur if:

- The UCF column is empty, but the GRC column contains an entry. In this case, the entity is no longer provided by UCF. The ServiceNow system responds by deactivating the entity in GRC, making it unavailable for any control test definitions that previously used it.
- The GRC column is empty, and the UCF column contains an entry. In this case, the download file contains a new entity that is added to GRC during the update.
- Both the UCF column and the GRC column contain entries. In this case, the entity must be updated from UCF to GRC.

Differences between UCF and GRC		
Item	UCF	GRC
Control name	Establish and maintain a process to control patch management and flaw remediation.	Establish and maintain a process to control patch management.
Control name	Patch software and update firmware.	Patch software.
Control name	Establish idle session termination and logout capabilities.	Establish idle session termination capabilities.
Control name	Establish and maintain a security testing policy and procedures.	Establish and maintain a security testing policy.
Control name	Establish and maintain logging and monitoring operations.	Establish and maintain logging and monitoring operations..

7. To update a new version of a document, select the check box on the card and click Import into GRC.

If approval is required, the system sends your request to users with the `grc_executive_approver` role, who can either approve or deny the request. The system moves approved content to the appropriate

GRC tables. If earlier versions of the document exist in the database, GRC increments the Version field on the new record and attaches it to the control test definitions, policies, and risks that use it.

8. View all previous versions of a source in the Other versions related list for records in the following tables:
  - Authoritative Source [grc\_authoritative\_source]
  - Authoritative Source Content [grc\_authoritative\_src\_content]
  - Control [grc\_control]

#### *Configure an automatic UCF download - Legacy*

When the GRC plugin is activated, the system creates a scheduled job called Notify GRC Admin new UCF is available. By default, this job is configured to check for new UCF authority documents each Monday.

When updates are downloaded, an event called grc.update sends an email notification to users with the grc\_admin role, advising them of the action. The administrator then reviews the changes before requesting updates to GRC. If the system is configured to require approval, all import requests are reviewed by users with the grc\_executive\_approver role, who can approve or reject the requested changes.

To allow this job to run and download UCF updates automatically:

1. Navigate to GRC > Administration > Properties
2. Set Enable automatic download to Yes.

## GRC citations imported from UCF - Legacy

You can download and import citations from a Unified Compliance Framework (UCF) authority document.

---

**Note:** For more information on Unified Compliance Framework (UCF), see <https://www.unifiedcompliance.com/>.

---

In UCF terminology, a citation record is referred to as an *instance of guidance*. Each guidance instance has a unique reference number attached to it that groups one or more instances into a *citation*. When you import a UCF authority document into the GRC application, the system lists them by their reference numbers. UCF citations are imported into the Authoritative Source Content [grc\_authoritative\_src\_content] table and can have duplicate reference numbers. For a description of fields in the Citation form not related to a UCF import, see [Create a GRC citation - Legacy](#) on page 204 . For details about importing citations, see [UCF authority document import process - Legacy](#) on page 235.



---

**Warning:** Fields imported from UCF are read-only, and their values should be protected for data continuity and accuracy. *Do not* customize fields to allow UCF data to be edited. Use the Additional information field to display any additional details or specifications for this UCF entity that are unique to your organization, while preserving the original citation from UCF.

---

< **Citation - Sched 1 ¶ 115** 
 Update Delete ↑ ↓

* Name	<input type="text" value="Sched 1 ¶ 115"/>	Type	<input type="text" value="-- None --"/>
Reference	<input type="text" value="Sched 1 ¶ 115"/>	Pertinent	<input checked="" type="checkbox"/>
Authority Document	<input type="text" value="Australia CLERP"/>		
Source	<input type="text" value="UCF"/>		
Source Id	<input type="text" value="0014673"/>		
Source Version	<input type="text" value="2013-06-19"/>		
Guidance	During annual meetings, voting shareholders must be able to submit questions to the auditor or audit firm that are relevant to the content of the auditor's report or the conducting of the financial audit. The list of questions being asked to the auditor must be available to all annual meeting attendees.		
Additional Information			

Update
Delete

**Related Links**

[Add related to](#)

[Add related from](#)

[View relationships](#)

Controls (1)
Policies
Related to
Related from
Other Versions

☰
Controls
New
Edit...

Go to

◀◀
◀

▶
▶▶
□

🔍 Citation = Sched 1 ¶ 115 > Control Active = true

	Control	Connected by
<input type="checkbox"/>	<div style="display: flex; align-items: center; gap: 5px;"> <span style="border: 1px solid #ccc; border-radius: 50%; padding: 2px 5px;">i</span> <span style="font-size: 0.9em;">Review the conclusions of the work papers and audit reports.</span> </div>	<span>(empty)</span>

Actions on selected rows...

◀◀
◀

▶
▶▶

Table 106: UCF fields in a citation form

Field	Description
Reference	UCF reference number for this citation. Duplicate reference numbers are possible in UCF data.
Name	Not used for UCF citations
Source	Source of the data for this citation. UCF is the source of all citations imported from UCF authority documents.
Source ID	Internal unique UCF identifier of the citation guidance for this citation.
Source version	Version of the UCF authority document that is the source file for this citation. Previous versions of this citation are listed in the Other versions related list.
Type	Type of citation created. This is an optional field and is not used for any processing. You can use the value in this field in reports or to query for records of a specific type.
Authority document	Name of the UCF authority document for this citation. When you import UCF authority documents, the system completes this field with the appropriate authority document.
Pertinent	Indicates if this citation is relevant to your organization. By default, this check box is selected and has a value of True. Clear this check box to mark this citation as not pertinent to your organization and to prevent it from appearing in compliance reporting. Components marked as <i>not pertinent</i> are unavailable for the <a href="#">calculated links</a> that enable results to rollup for any GRC hierarchy.
Version	[Read-only] Version number for previous versions of this citation. This value is a simple integer that is incremented by the system each time the UCF citation is updated. This number is not the same as the UCF Source version. The Version field is hidden when the current version of the record is displayed. You can view all available versions by selecting records from the Other Versions related list. For more information, see <a href="#">GRC citations imported from UCF - Legacy</a> on page 253 .
Guidance	[Read-only] The citation imported as UCF Citation Guidance. Since multiple UCF citation records can have the same reference number, this string identifies this specific citation.

Field	Description
Additional information	Information of any type that is pertinent to this citation This field is not used for any processing.

### UCF citation versions

The ServiceNow system creates a new version of the citation each time a new UCF authority document is imported into GRC. When a new version is created, the system adds the previous version to the Other versions related list in the Control form. These records are used for reference only and provide a history of how each previous version of the UCF citation was used. New control tests run against the current control version only. Only the latest versions of citations appear in lists.

### Deactivating and Deleting citations

You cannot delete a GRC record that has a linked dependency to another GRC record. The Delete button appears in records and record lists, but only *deactivates* the entity rather than removing it from the system. Deactivation clears the Pertinent check box in the record, which removes any links to other GRC entities. By default, deactivated records are filtered out of related lists. Manually created GRC records with no linked dependencies can be completely deleted from the system. UCF records imported into GRC tables can only be deactivated. Only users with the admin role can deactivate or delete GRC records.

### UCF download background processes and status - Legacy

The UCF download process runs in the background to automatically prepare the UCF data for selection as GRC authoritative content.

- Downloads and unpacks the UCF ZIP archive.
- Loads the unpacked files into temporary staging tables.
- Compares downloaded UCF files to any previous GRC updates.
- Creates staging tables used for calculations only.

The ServiceNow system creates staging tables to hold UCF data before moving it into the GRC target tables:

**Table 107: UCF staging tables**

Staging Table	Target Table	Description
GRC UCF Authority Document [grc_ucf_authority_document]	Authority Document [grc_authoritative_source]	Stores authority documents in GRC.
GRC UCF Citation Mapping [grc_ucf_citation_mapping]	Citation [grc_authoritative_src_content]	Stores citation data in GRC.
GRC UCF Control [grc_ucf_control]	Control [grc_control]	Stores controls in GRC.
GRC UCF Update Status [grc_ucf_update_status]	No mapped table in GRC.	Stores the current progress of a UCF update. The instance uses this data to display the correct status of an import to one or more logged-in users and to prevent interruption of the import process.



Staging Table	Target Table	Description
GRC UCF Filter [grc_ucf_filter]	No mapped table in GRC	Stores the number of documents in each UCF group. These are the values displayed for each group in the filter screen.

### UCF download status

The details of the UCF download are stored in the UCF Download Status [grc\_ucf\_download\_status] table.

Navigate to GRC > Administration > UCF Download Status .

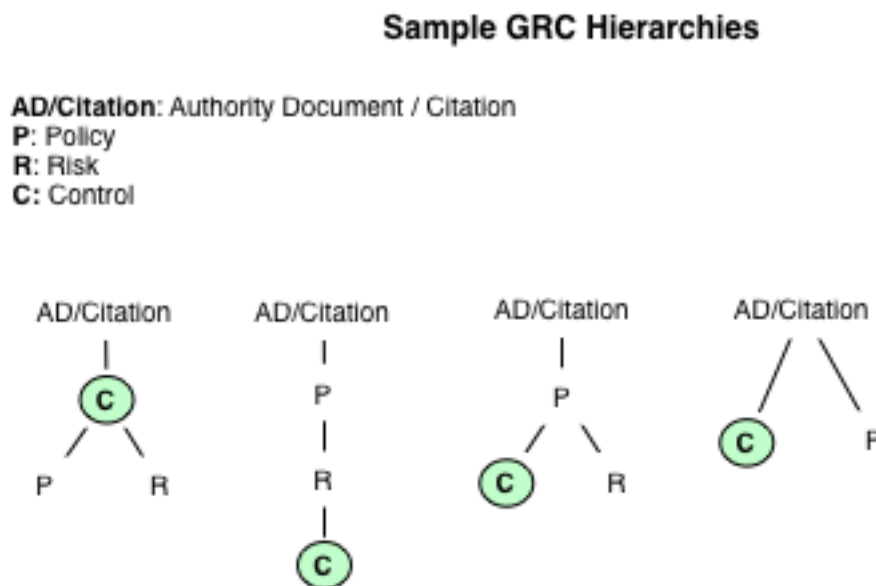
UCF Download Status					Go to	Name	Search	1 to 14 of 14	
All									
		↓ Name	Group	Message	Value				
<input type="checkbox"/>	<a href="#">Build filter table</a>	load_UCF	Table built successfully	Finished					
<input type="checkbox"/>	<a href="#">Compare against GRC</a>	load_UCF	Up to date: 5; Update available: 4; Not ...	Finished					
<input type="checkbox"/>	<a href="#">Connect to server</a>	load_UCF	Connected successfully	Finished					
<input type="checkbox"/>	<a href="#">Current step</a>	load_UCF		6					
<input type="checkbox"/>	<a href="#">Current UCF file name</a>	load_UCF		14Q4_Final_XML.zip					
<input type="checkbox"/>	<a href="#">Current UCF version</a>	load_UCF		Quarter 4, 2014					
<input type="checkbox"/>	<a href="#">Download Authority Documents</a>	load_UCF	Records downloaded: 682	Finished					
<input type="checkbox"/>	<a href="#">Download Citations</a>	load_UCF	Records downloaded: 100146	Finished					
<input type="checkbox"/>	<a href="#">Download Controls</a>	load_UCF	Records downloaded: 9561	Finished					
<input type="checkbox"/>	<a href="#">Message</a>	load_UCF		Downloaded successfully					
<input type="checkbox"/>	<a href="#">Started by</a>	load_UCF		System Administrator					
<input type="checkbox"/>	<a href="#">Status</a>	load_UCF		Finished					
<input type="checkbox"/>	<a href="#">Time finished</a>	load_UCF		Sun Jan 11 19:22:34 PST 2015					
<input type="checkbox"/>	<a href="#">Time started</a>	load_UCF		Sun Jan 11 19:15:19 PST 2015					
<input type="checkbox"/>	Actions on selected rows...				1 to 14 of 14				

## Calculated links between GRC tables - Legacy

The links between authority documents, policies, controls, and risks can take a number of different paths, depending on your organization's requirements.

GRC supports any hierarchy you create by establishing many-to-many relationships between all the tables involved and using these relationships to create *calculated links* between elements. Calculated links are indirect links between elements that aid in reporting on authority documents by rolling up results from control tests. Calculated links are created automatically as you add direct links between elements and managed dynamically as you edit existing links in your hierarchy.

Figure 10: Sample GRC element hierarchies



## How GRC calculated links work - Legacy

An organization can use GRC calculated links to view connections between GRC records in a hierarchy that are not directly connected.

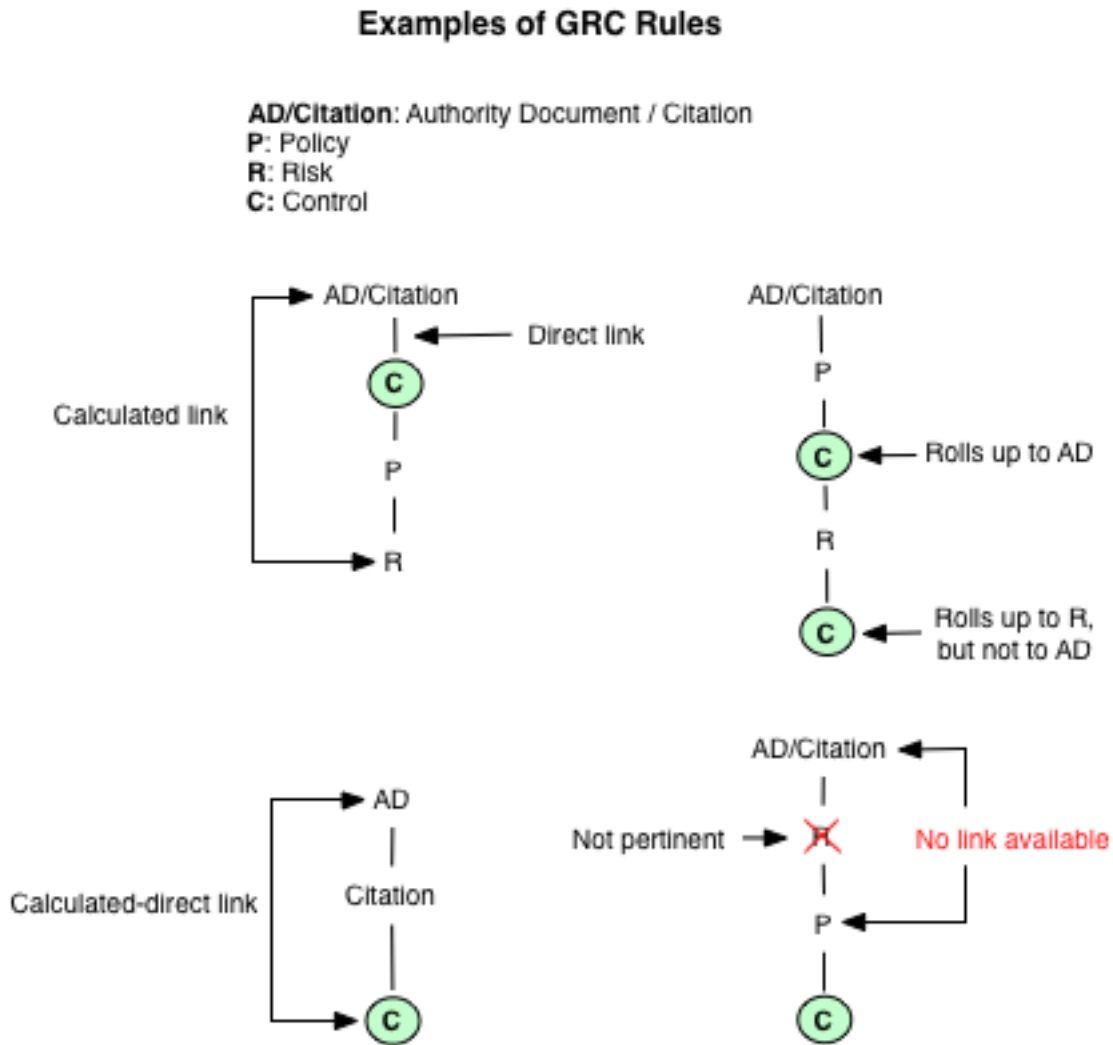
GRC provides a table structure that maintains all possible combinations of links and then links everything together in the hierarchy you create.

GRC uses these rules when calculating links:

- Links are calculated between authority documents, and policies, risks, and controls. These links are shown in forms, together with the method of connection, in addition to other related lists.
- Links are calculated between controls, policies, and risks when rolling up control test results for authority documents, policies, and risks.
- Authority documents and citations are at the top of the hierarchy. Control test definitions and control test instances provide data about the number of passing and failing control tests at all levels. Controls, policies, and risks are equal components. Links can go in any direction between these elements.
- An authority document and its citations are treated as a single entity. A direct link to an authority document is the same as a direct link to the related citations. Components linked directly to citations are linked to the authority document with the *calculated - direct* link, created specifically for this purpose. Calculated links are only created to the authority document and *not* to the citations.

- The system only creates links between components configured as pertinent. See [Create a GRC citation - Legacy](#) on page 204. For example, if an authority document, a risk, and a policy are all linked together, and the risk is configured as not pertinent, the system cannot link the policy to the authority document when rolling up data for reporting.
- Users cannot manually delete calculated links.

Figure 11: GRC element linking rules



## GRC tables for calculated linking - Legacy

These tables store all the possible links defined in the system between GRC components.

The Calculated and Connected by columns contain information about the indirect links between records that GRC creates for your hierarchy. The Pertinent column in each table determines if the components are available for linking. When you mark a component in a hierarchy as not pertinent, the system considers the direct links on either side of that component as not pertinent and does not establish an indirect link through that node.

Table 108: Calculated linking tables

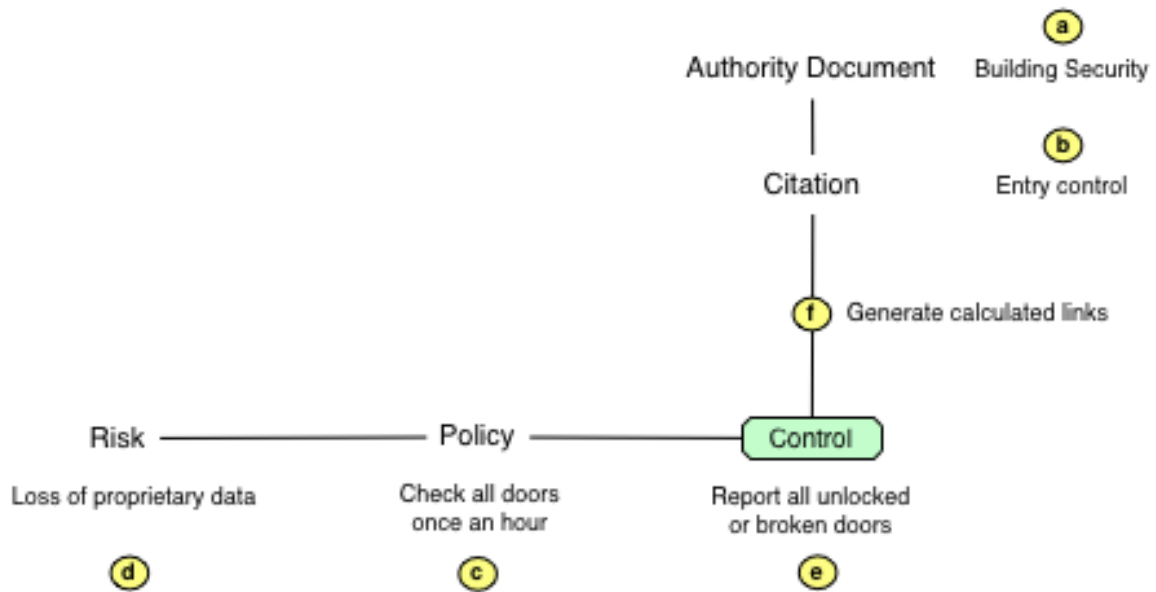
Table	Description
Control Authoritative Source [m2m_control_authoritative_source]	Stores the reference link between a control and an authority document.
Control Authoritative Source Content [m2m_control_auth_src_content]	Stores the reference link between a control and a citation.
Policy Control [m2m_control_policy]	Stores the reference link between a control and a policy.
Policy Authoritative Source Content [m2m_policy_auth_scr_content]	Stores the reference link between a policy and a citation.
Risk Control [m2m_risk_control]	Stores the reference link between a risk and a control.
Risk Policy [m2m_risk_policy]	Stores the reference link between a risk and a policy.
Policy Authoritative Source [m2m_policy_authoritative_source]	Stores the reference link between a policy and an authority document.
Risk Authoritative Source [m2m_risk_authoritative_source]	Stores the reference link between a risk and an authority document.

## GRC calculated links example - Legacy

GRC establishes both direct and indirect links between GRC records that enable it to function with any hierarchy, regardless of the order in which the elements appear.

In this example hierarchy, an authority document manages building security regulations using a policy that defines the potential risk and a control to ensure that the policy is being followed. The goal is to report on authority documents by rolling up the results of failed and passed control tests through policies and risks. Procedures have been put into place to prevent loss of company property and data from unauthorized entry into company buildings. Security personnel are directed to check the doors once an hour and report any issues they find. For the purposes of this example, the authority document (a) is the first element created, and the control (e) is the last element. When the link (f) is created between the citations and the control, the system generates the calculated links needed to roll up data properly through the hierarchy. These links function the same with controls, risks, and policies in other configurations.

**Figure 12: GRC calculated links example**



### Process for linking elements

The best method for linking together the elements of a GRC hierarchy is to create each element from within the record of another element. In this example, the first task is to create the authority document and its citations, and then create a policy linked to a risk and a control. Finally, the citations and the control are linked, which generates the calculated links between the authority document and the other elements in the hierarchy. Remember that all elements must be configured as *pertinent* for the system to complete the linking process.

#### *Create a GRC authority document manually - Legacy*

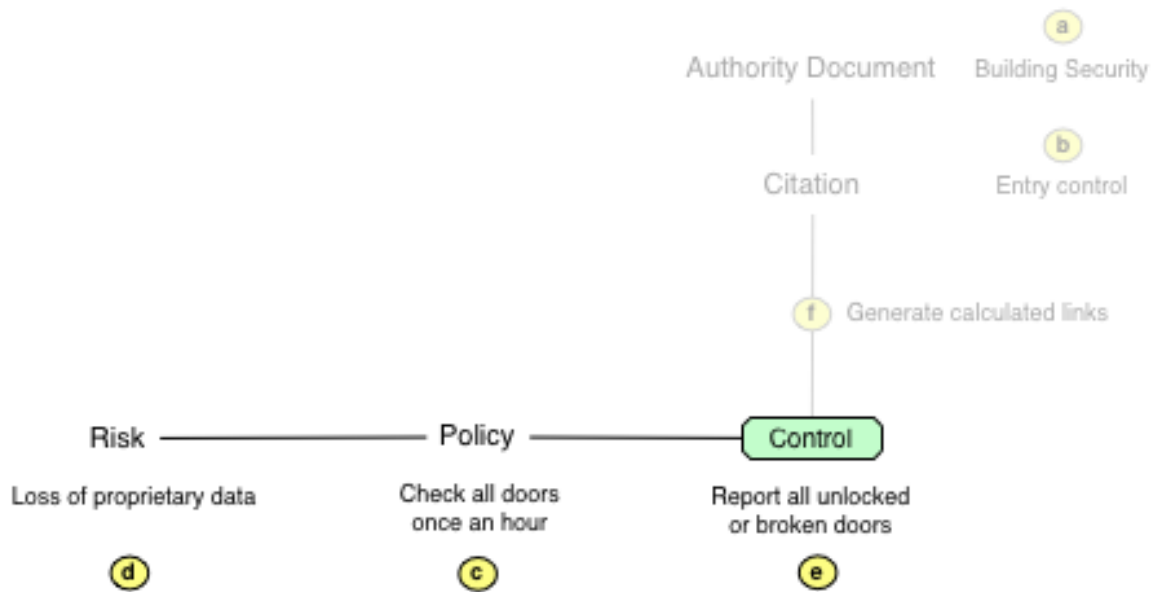
Create an authority document.

1. Navigate to GRC Authority Documents Authority Documents .
2. Click New.
3. Fill in the fields on the form, as appropriate.
4. Right-click in the header bar and select Save from the context menu.
5. In the Citations related list, click New.
6. Fill in the fields on the form, as appropriate.
7. Click Submit.

#### *Create a GRC policy - Legacy*

Create a policy (c), then link it to a risk (d) and a control (e).

**Figure 13: GRC calculated links example for policies**



1. Navigate to GRC Policies .
2. Click New.
3. Type a short description that identifies this policy, such as Check all doors once an hour.
4. Make sure the Pertinent check box is selected.
5. Save the record.
6. In the Risks related list, click New.
7. Complete these fields:
  - Risk name: *Loss of proprietary data*
  - Pertinent: Selected

The screenshot shows a ServiceNow Risk form. At the top, there is a navigation bar with a back arrow, a hamburger menu, the text "Risk", and icons for edit, help, settings, submit, and up. The form fields are arranged in two columns. The left column contains: Risk ID (RISK0002003), Name (Loss of proprietary data), Significance (-- None --), Likelihood (-- None --), Recommended approach (empty), Pertinent (checked), Description (empty), and Additional information (empty). The right column contains: State (Known), Category (-- None --), Compliance (0), Non compliance (0), and Applies to (empty). A Submit button is located at the bottom left of the form area.

Risk ID	RISK0002003	State	Known
* Name	Loss of proprietary data	Category	-- None --
Significance	-- None --	Compliance	0
Likelihood	-- None --	Non compliance	0
Recommended approach		Applies to	(empty)
Pertinent	<input checked="" type="checkbox"/>		
Description			
Additional information			

8. Click Submit.

The Policy form appears.

9. In the Controls related list, click New.

10. Complete these fields:

- Name: *Report all unlocked or broken doors*
- State: *Active*
- Pertinent: Selected



< ☰ Control 📎 ? ⚙️ Submit ↑

Control ID	<input type="text" value="CTRL0002069"/>	State	<input type="text" value="Active"/>
Owning group	<input type="text"/> 🔍	Classification	<input type="text" value="-- None --"/>
Owner	<input type="text"/> 🔍	Purpose	<input type="text" value="-- None --"/>
Owner delegate	<input type="text"/> 🔍	Control frequency	<input type="text" value="-- None --"/>
Pertinent	<input checked="" type="checkbox"/>	Compliance	<input type="text" value="0"/>
Key control	<input type="checkbox"/>	Non compliance	<input type="text" value="0"/>
Name	<input type="text" value="Report all unlocked or broken doors"/>		
Description	<input type="text"/>		
Additional information	<input type="text"/>		

Submit

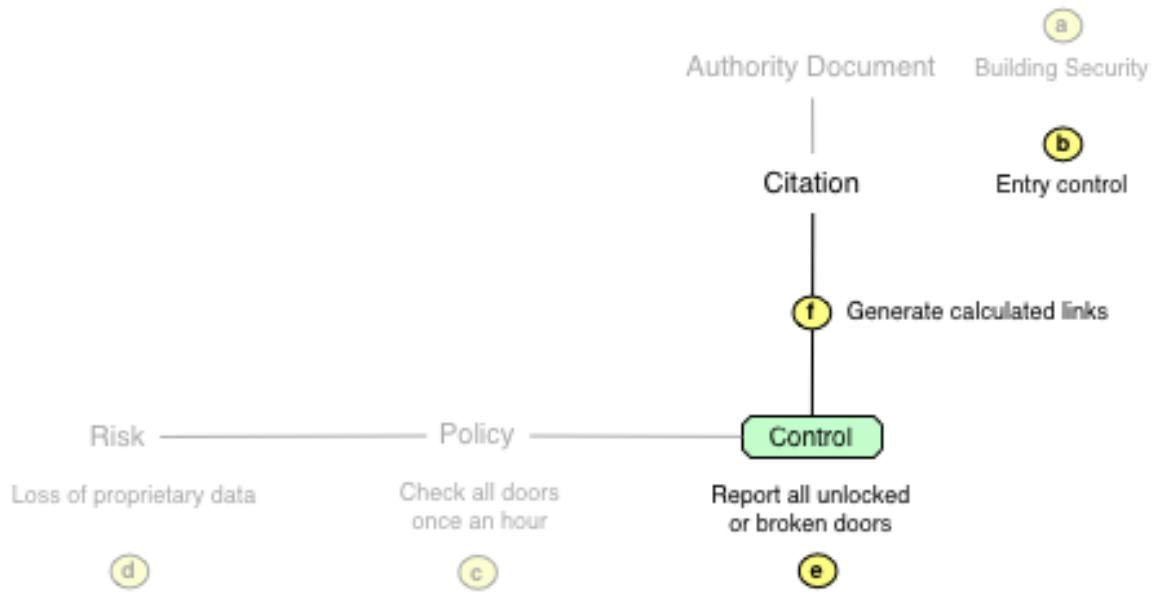
**11. Click Submit.**

The Policy form appears, displaying the linked risk and control in related lists. The value in the Connected by column is (empty), indicating that direct links exist between this policy and the risk and control.

The screenshot displays two views of a policy: 'Risks' and 'Controls'. Both views show a table with one row. In the 'Risks' view, the risk is 'Loss of proprietary data' and the 'Connected by' field is '(empty)'. In the 'Controls' view, the control is 'Report all unlocked or broken doors' and the 'Connected by' field is also '(empty)'. A red box highlights the '(empty)' text in both views, with a red arrow pointing to it from a text box that reads: 'Indicates that links to this policy are direct and not calculated'.

#### *Generate calculated links - Legacy*

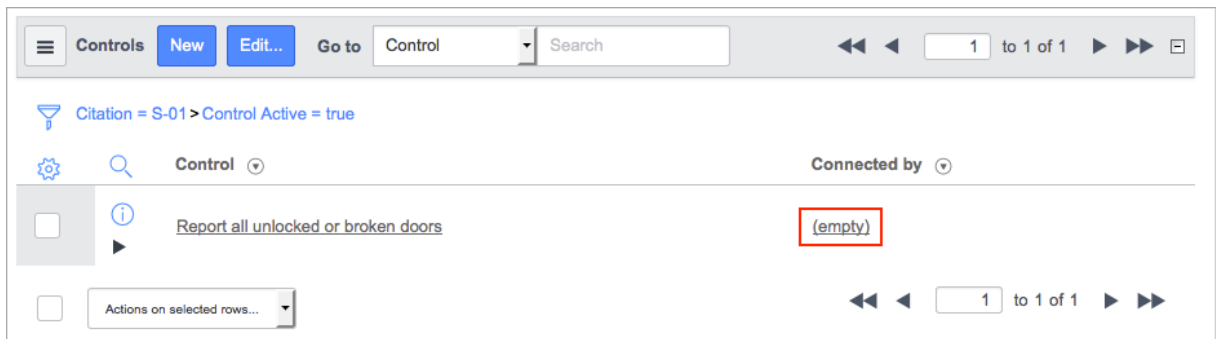
To generate the calculated links from the authority document to the other elements in the hierarchy, create the link (f) from the citation (b) to the control (e).



**Figure 14: GRC calculated links generation, example hierarchy**

1. Navigate to GRC Authority Documents Authority Documents .
2. Open the Building Security record.
3. In the Citations related list, select the S-01 record.
4. In the S-01 citation record, click Edit in the Controls related list.
5. Select the control called Report all unlocked or broken doors that was linked to the policy in the previous section.
6. Click Save.
7. To view the link information look at the Connected by column, which shows the path between elements connected by calculated links.

The value in the Connected by column in the Control related list is (empty), indicating that a direct link exists between this citation and the control, and no calculated link was created.



8. Navigate to GRC Authority Documents Authority Documents and open the Building Security record.
9. In the related list for Controls, Policies, or Risks, point at the value in the Connected by column.  
The system displays the complete connection path for the calculated link in a pop-up box.

**Controls** [New](#) [Edit...](#) Go to **Control** Search 1 to 1 of 1

Authority Document = Building Security > Control Active = true

	Control	Connected by
<input type="checkbox"/>	<a href="#">Report all unlocked or broken doors</a>	<a href="#">Via S-01 'Entry control'</a>

Actions on selected rows... 1 to 1 of 1

---

**Policies** [New](#) [Edit...](#) Go to **Policy** Search 1 to 1 of 1

Authority Document = Building Security

	Policy	Class	Connected by
<input type="checkbox"/>	<a href="#">Check all doors once an hour</a>	Policy	Via S-01 'Entry control' Via CTRL0002069...

Actions on selected rows... 1 to 1 of 1

**Via S-01 'Entry control' Via CTRL0002069 'Report all unlocked or broken doors'**

---

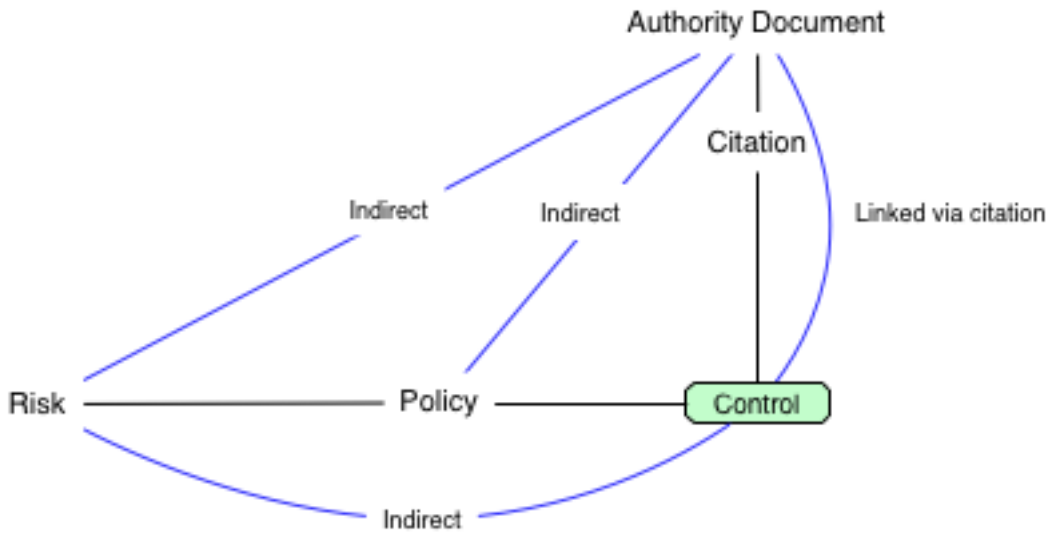
**Risks** [New](#) [Edit...](#) Go to **Risk** Search 1 to 1 of 1

Authority Document = Building Security

	Risk	Connected by
<input type="checkbox"/>	<a href="#">Loss of proprietary data</a>	<a href="#">Via S-01 'Entry control' Via CTRL0002069...</a>

Actions on selected rows... 1 to 1 of 1

In this example, GRC automatically creates these calculated links:



- To view the link record, click the value in the Connected by column.

The record displays the elements that are linked, the calculated link type, and the connection path. In this example, the authority document is linked to the control by a special link called a *calculated direct* link, expressed here as *Linked via content*. This type of link is created only when an authority document is linked to another element through the citation.

< **Control Authority Document - Building Security**

🔗 ? ⚙️
Update
↑ ↓

Authority Document  🔍 ⓘ

Control  🔍 ⓘ

Update

Calculated Linked via content

Connected by Via S-01 'Entry control'

The connection paths are as follows:

**Table 109: Calculated links**

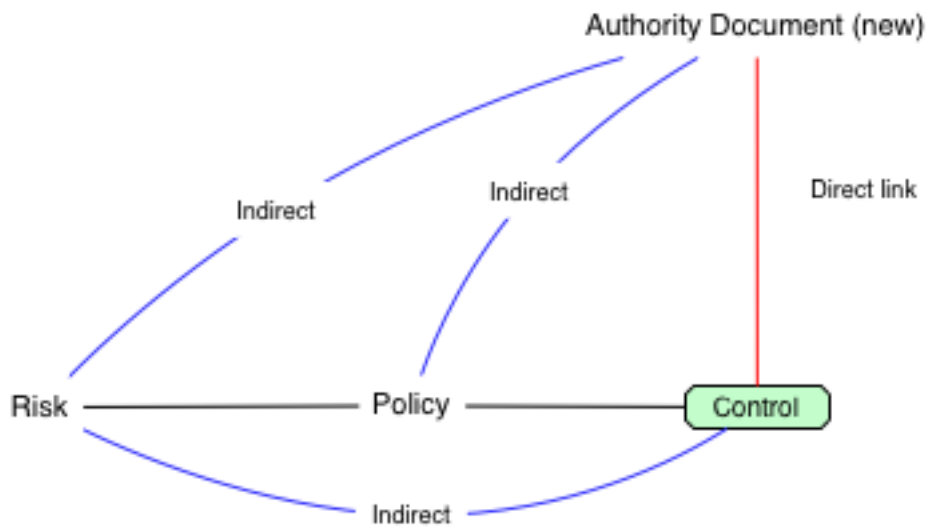
Elements linked	Calculated link	Connection path
AS - C	Linked via content	Via the citation

Elements linked	Calculated link	Connection path
AS - P	Indirect link	Via the citation and the control
AS - R	Indirect link	Via the citation, the control, and the policy
R - C	Indirect link	Via the policy

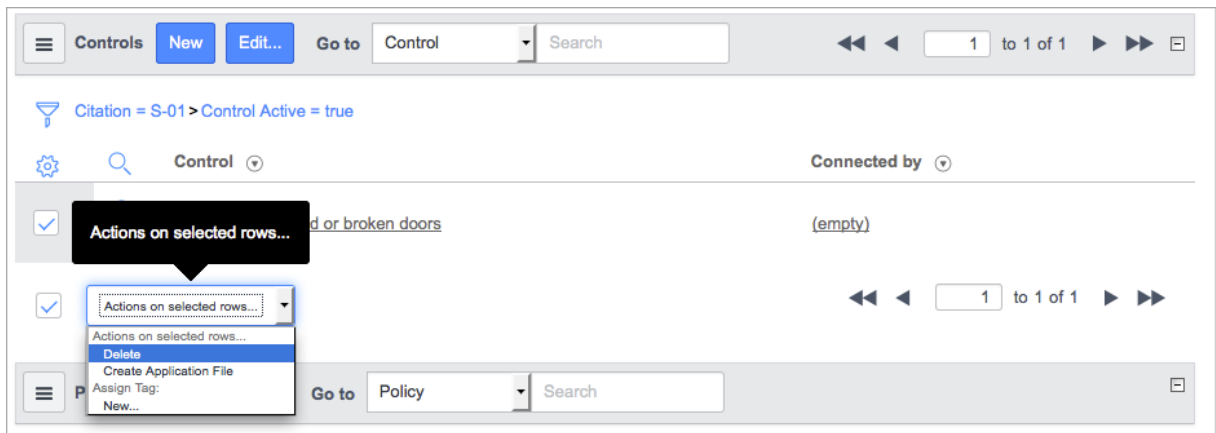
### *Redirect the link - Legacy*

Delete the direct link to the control from the citation and link the control directly to a new authority document.

GRC redraws all the indirect links correctly within the new hierarchy.



1. Navigate to GRC Authority Documents Authority Documents .
2. Open the Building Security record.
3. In the Citations related list, select the S-01 record.
4. In the citation record, select the Controls related list.
5. Delete the Report all unlocked or broken doors control from the list, using the command in the Actions choice list.



Breaking this link deletes all the calculated links GRC created between the authority document and the other entities in the hierarchy.

6. Navigate to GRC Authority Documents Authority Documents .
7. Create a new record called Datacenter Security.
8. Make sure the record is Pertinent.
9. Right-click in the header bar and select Save from the context menu.
10. In the Controls related list, click Edit.
11. Select the Report all unlocked or broken doors control and click Save.

The system creates calculated links from the new authority document to the appropriate elements and displays the links in the related lists. The link between the authority document and the control is now a direct link and does not need to be calculated. Point at a value in the Connected by column to display the complete path in a pop-up window.



The screenshot displays the ServiceNow GRC interface for an Authority Document titled "Datacenter Security". It is divided into three main sections: Policies, Risks, and Controls.

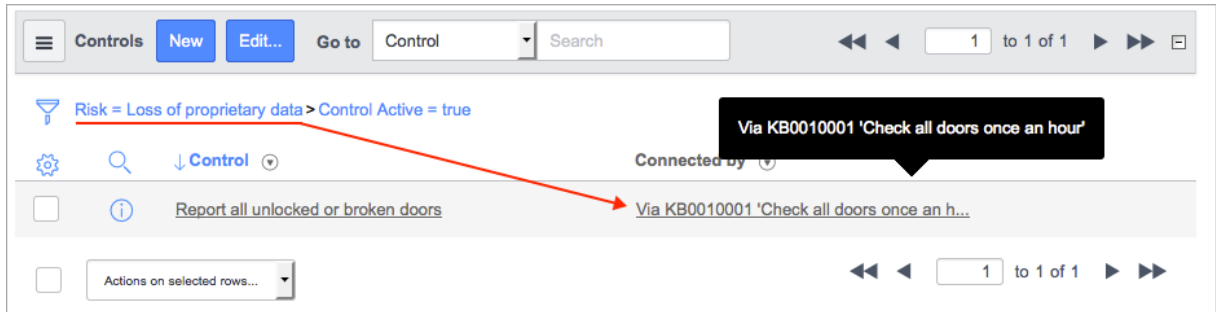
- Policies Section:** Shows a table with columns for Policy, Class, and Connected by. One policy is listed: "Check all doors once an hour" (Class: Policy). The "Connected by" field contains the text "Via CTRL0002069 'Report all unlocked or ...'".
- Risks Section:** Shows a table with columns for Risk and Connected by. One risk is listed: "Loss of proprietary data" (Class: Risk). The "Connected by" field contains the text "Via CTRL0002069 'Report all unlocked or ...'".
- Controls Section:** Shows a table with columns for Control and Connected by. One control is listed: "Report all unlocked or broken doors" (Class: Control). The "Connected by" field is empty.

Annotations in the image:

- A red box labeled "New calculated links" has arrows pointing to the "Connected by" fields in the Policies and Risks sections.
- A black callout box contains the text: "Via CTRL0002069 'Report all unlocked or broken doors' Via KB0010001 'Check all doors once an hour'".
- A red box labeled "Direct link between authoritative source and control" has an arrow pointing to the "(empty)" field in the Controls section.

- To see the link between the risk and the control, navigate to **GRC Risks** and select the **Loss of proprietary data** record.

Notice that the value in the **Connected by** column in the **Controls** related list shows an indirect calculated link to the risk through the policy.



The connection paths are as follows:

**Table 110: Recalculated links**

Elements linked	Calculated link	Connection path
AS - P	Indirect link	Via the control
AS - R	Indirect link	Via the policy and the control
R - C	Indirect link	Via the policy

## Risk Management overview - Legacy

Risk management enables an organization to quickly identify and quantify the impact that loss events affecting various business processes and items (such as facilities, business services, and vendors) pose to the organization. A risk is a definition of the possible consequence of failing to comply with a policy.

Risks are rated on criteria that can be used to calculate a risk approach. The risk approach calculation is based on risk approach rules that typically use the values contained in the Significance and Likelihood fields in the Risk Criteria [grc\_risk\_criteria] table. This table contains a Display value field to allow for text values and a weighting, which can be used to define the risk approach rules. After the risks are defined, they can be associated with controls to identify how they are being mitigated.

By utilizing risk and profiles, organizations can coordinate the risk assessment process to prioritize the order and frequency of risk assessments, control testing, and periodic audits against each entity.

- Ensure that the settings for Risk Criteria, Risk Criteria Thresholds, and Properties are correct based on the needs of your organization. Modify if necessary.

2. Create Profile Types to group common Profiles with similar risks together for easier assessment.
3. Generate profiles from Profile Types, or create Profiles manually.
4. Create Risk Definitions to define a set of baseline risks that should be assessed across the organization.
5. Assign Risk Definitions to Profile Types, and Generate Risks from Definitions, or generate Risks manually.
6. Determine the appropriate risk response (for example, Accept, Avoid, Mitigate, or Transfer), and document the justification for the response.
7. Assign and complete Remediation Tasks to ensure that risk mitigation efforts are implemented.
8. Utilize the Governance, Risk, and Compliance (GRC) application to track risk mitigation efforts by relating a risk to controls or policies which mitigate the risk.

## Migrate from Legacy Risk

A migration tool is provided to migrate Legacy Risk risks, risk definitions, risk/task relationships, and/or control/risk relationships to the new GRC applications.

Role required: sn\_compliance.admin or sn\_risk.admin

---

**Note:** Customers currently using Legacy Risk [com.sn\_risk] are not required to activate the plugin and migrate to the new functionality.

---

1. Navigate to Risk Administration Migration .
2. Select the items to migrate.
3. Click Migrate.  
A summary of successfully migrated items is shown.

Figure 15: Items successfully

Risk	
 Risks (376)	Successfully migrated
 Risk/task associations (0)	Successfully migrated

migrated

## Create a profile type - Legacy

Profile types are similar to a category in that they group like profiles together. However, profile types are more powerful than categories, because business logic automates the identification of all potential profiles in the system that meet the profile type conditions.

1. Navigate to Risk Profile Types Create New .
2. Click New.

3. Complete the Profile Type form using the following table.

**Table 111: Fields on the Profile Type form**

Name	Description
Name*	Sets the name of the Profile Type.
Table*	Select the table from which the Profile Type conditions identify the records to create profiles.
Owner field*	Select the field on the table which contains an owner. For all profiles created, the owner of the profile is set based on the field selected here, regardless of whether or not it is the true owner of the entity. For example, if the profile is for an asset, the owner might be set to the asset manager instead of the owner using the asset.
Empty owner	Determines the appropriate action if the owner field on the table is empty. The following choices are available. <ul style="list-style-type: none"> <li>• Create—creates a profile with an empty owner field.</li> <li>• Do Not Create—does not create a profile for a record that does not have an owner specified in the owner field.</li> <li>• Use Default—creates a profile assigned to the user identified as the default owner.</li> </ul>
Default Owner*	Only available if the Empty owner field is set to Use Default. Select the owner that should be assigned to Profiles that have an empty Owner field.
Condition	Set filter conditions to restrict which profiles belong to a specific profile type.
Description	Sets an explanation of the Profile Type with any additional information about the Profile Type that a user may find helpful.

---

**Note:** \* indicates a mandatory field.

---

4. Click Submit.

## Generate a profile from a profile type - Legacy

Profiles are not automatically generated by creating the Profile Type; they must be generated manually.

1. Navigate to the Profile Type [Risk Profile Types All Profile Types](#) and open the Profile Type record.

2. Ensure that all the information entered on the form is correct, and add or modify any conditions if necessary.
3. Click Generate Profiles in the Related Links.  
A security message appears.
4. If the conditions are correct, click OK. If the conditions or form need edited, click Cancel.  
A profile is generated for every matching record found. The generated profile populates the Profiles Related List.

## Create a profile - Legacy

Profiles are the records that aggregate GRC information related to a specific item. Profiles can exist for any particular item such as a business service, vendor, demand, software, contract, or any other record in the system. An item can only have one profile, but it can belong to many profile types. Profiles cannot be created for items that do not have a record in a table.

---

**Note:** If a new record is created, a new profile is not automatically generated. A new profile can be generated from the Related Link or from the profile type form. A new profile can also be created manually. If the profile is created manually and the new profile meets the conditions for a profile type, it is automatically related to that profile type.

---

1. Navigate to Risk Profiles Create New , or navigate to Risk Profiles Create New My Profiles or All Profiles
2. Click New.
3. Complete the Profile form using the following table.

**Table 112: Fields on the Profile form**

Name	Description
Name*	Sets the name of the Profile. If empty, the name is set to the name of the record to which the Profile applies.
Owned by*	Select the owner of the Profile.
Applies to*	Select the table and the document to which the Profile applies.
Inherent Score	Read-only field on the form section for Risk. Reports the inherent risk to the organization prior to any corrective action or mitigation efforts. See Scoring Risk on Profiles.
Residual Score	Read-only field on the form section for Risk. Reports the residual risk to the organization prior to any corrective action or mitigation efforts. See Scoring Risk on Profiles.
Calculated Score	Read-only field on the form section for Risk. Reports the actual score of the risk to the organization based on the inherent and residual scores and the compliance to controls used to mitigate the risks. See Scoring Risk on Profiles.

---

**Note:** \* indicates a mandatory field.

---

- Click Submit.

## Profile scoring - Legacy

The inherent, residual, and calculated scores on a profile are read-only and provided so you can quickly assess the risk of an item identifying threats and areas of non-compliance.

Each score is an average of the respective scores of all risks related to the profile. For example, if you have five risks related to a profile, the inherent score of the profile is the average of the five inherent scores of the risks.

If the score field for a risk is empty, the score counts as 0 when calculating the average score for a profile.

## Create a risk definition - Legacy

Risk definitions act as a template for creating risks, but also allow you to group like risks together. They automate the process of creating and assigning risks to items that the risk relates to.

- Navigate to Risk Definitions Create New .  
You can also create Definitions by clicking New in the Risk Definitions related list on the Profile Type form.
- Fill in the fields on the form, as appropriate.

Name	Description
Name*	Sets the name of the Risk Definition, as well as the names of Risks related to the definition.
Category*	Choose the category of risks related to this definition. Choose from the following options. <ul style="list-style-type: none"> <li>IT</li> <li>Reputational</li> <li>Operational</li> <li>Financial</li> <li>Legal</li> </ul>
Inherent significance	Define the inherent significance of the risks related to this definition if one did occur.
Inherent likelihood	Define the inherent likelihood that the risks related to this definition will occur.
Description*	Description of the Risks related to this definition.
Additional Information	Add any information that may need to be included with the risks related to the definition.

---

**Note:** \* indicates a mandatory field.

---

- Click Submit.

## Relate a risk definition to a profile type - Legacy

After a risk definition is created, it can be related to a profile type to generate a risk.

1. Navigate to Risk All Profile Types Select a Profile Type .
2. Navigate to the Risk Definitions related list, and click Edit.  
You can also create a new risk definition from the related list by clicking New.
3. Add all Risk Definitions that apply to this Profile Type. Click Save to relate the chosen Risk Definitions to the Profile Type, or Cancel to return to the Profile Type form without relating the chosen Definitions.
4. Select Generate Risks from Definitions in the Profile Type form's Related Links.

The following message displays:

Are you sure you want to generate Risks from all Definitions associated with this Profile Type?

5. Click OK to create a Risk from each Definition for every Profile in the Profile Type. Click Cancel to return to the form and edit the Risk Definitions associated with the Profile Type.

## Create a risk - Legacy

Risks are the specific records used to document and assess the likelihood and significance of a risk.

Tracking risks that exist throughout your organization is vital to ensure appropriate action is taken to reduce operational risks, where possible.

1. Choose one of the following options.
  - Generate Risks from Definitions using the related link on the Profile Type form. For more information, see [Create Risk Definitions](#).
  - Create Risks manually by navigating to Risk Risk Register Create New .
  - Navigate to My Risks or All Risks and select New
  - Select New in the Risk related list on the Profile form.
2. Fill in the fields on the form, as appropriate.

**Table 113: Risk form**

Name	Description
Risk ID	Read-only field that is automatically populated with a unique identification number.
Name*	Set the name of the Risk. Field is auto-populated if Risk is generated from a Definition, but can be changed without affecting the relationship between Risk and Risk Definition.
Owned by*	Set the owner of the Risk. The owner of the Risk can be different than the owner of the Profile.
Definition	Allows user to relate and auto-populate a Risk with information from a Risk Definition.

Name	Description
State	<p>Sets the state of the risk. You have the following options.</p> <ul style="list-style-type: none"> <li>• Known—The existence of the risk is known.</li> <li>• Open—The risk has been analyzed. This is the default value.</li> <li>• Issue—The risk has occurred.</li> <li>• Closed—The risk is no longer valid. For example, the risk was related to mainframes, but the organization no longer uses mainframes.</li> </ul>
Category	<p>Choose a category of risk which applies to the Profile. You have the following options.</p> <ul style="list-style-type: none"> <li>• IT</li> <li>• Reputational</li> <li>• Operational</li> <li>• Financial,</li> <li>• Legal</li> </ul> <p>Field is auto-populated if Risk is generated from a Definition.</p>
Profile	Relate the Risk to a specific profile.
Applies to	Select a table and a record from that table to identify the scope of the risk. Using this field will relate the risk to a profile for the record if one exists.
Pertinent	Indicator that shows if a risk document is relevant to your organization. By default, this check box is selected, and has a value of TRUE. Clear this check box to mark this risk as not pertinent to your organization, and to prevent it from appearing in compliance reporting. See <a href="#">Calculated links between GRC tables - Legacy</a> on page 259 .
Pertinent	Indicator that shows if a risk document is relevant to your organization. By default, this check box is selected, and has a value of TRUE. Clear this check box to mark this risk as not pertinent to your organization, and to prevent it from appearing in compliance reporting. See <a href="#">Calculated links between GRC tables - Legacy</a> on page 259.
Description	Describe the Risk and how it is a threat to the organization.
Additional Information	Detail any additional information that should be included with the risk record.



Name	Description
Inherent significance	Define the significance of the risk before any corrective action or mitigating efforts are applied. Field is auto-populated if Risk is generated from a Definition.
Inherent likelihood	Define the likelihood of risk occurrence before any corrective action or mitigating efforts are applied. Field is auto-populated if Risk is generated from a Definition.
Residual significance	Define the significance of the risk after corrective action or mitigating efforts are applied.
Residual likelihood	Define the likelihood a risk occurs after corrective action or mitigating efforts are applied.
Inherent Score	Read-only field that is the calculated score of inherent risk.  Inherent Score = Inherent Likelihood x Inherent Significance
Residual Score	Read-only field that is the calculated score of residual risk.  Inherent Score = Inherent Likelihood x Inherent Significance
Calculated Score	Read-only field that is the calculated based on the inherent score, residual score, and the compliance score of the controls related to the risk. For more information, see <a href="#">Score Risks</a> .
Response	Identify the response to a risk. You have the following options. <ul style="list-style-type: none"> <li>• Accept—accept the risk as is.</li> <li>• Avoid—avoid the risk, for example, by retiring a business service.</li> <li>• Mitigate—mitigate the risk through the implementation of controls.</li> <li>• Transfer—transfer or outsource the risk to a third-party.</li> </ul>
Justification	Detail, describe, and justify the Response.
Compliance	Read-only field that shows the percent compliance for the mitigation controls related to the risk. Only set if the Governance, Risk, and Compliance (GRC) plugin is activated.

Name	Description
Non compliance	Read-only field that shows the percent non-compliance for the mitigation controls related to the risk. Only set if the Governance, Risk, and Compliance (GRC) plugin is activated.

---

**Note:** \* indicates a mandatory field.

---

**3.** Click Submit.

Once a Risk is created, either manually or generated from a definition, it has a related list for Remediation that allows you to manage the remediation tasks associated with the risk. Additional related lists for Authority Documents, Controls, Policies, and Tasks appear on the risk record if the plugin Governance, Risk, and Compliance (GRC) is activated.

## Risk scoring - Legacy

The inherent and residual scores for a risk can be calculated using the risk criteria, likelihood, and significance.

Use the following calculations to score risks.

- Inherent Score = Inherent Likelihood x Inherent Significance
- Residual Score = Residual Likelihood x Residual Significance

Since the risk properties have maximum values for likelihood and significance set at 5 , the maximum inherent or residual score for a risk is 25. This can be changed by modifying the Risk Properties. See [Risk properties - Legacy](#) on page 285.

The maximum value for the inherent or residual score is 100. If the maximum value of their respective properties are changed to 10, the fields for scores are read-only, and can only be changed by modifying the inherent or residual, likelihood or significance.

The calculated score for a risk is read-only allowing you to quickly assess a risk, and identify threats and areas of non-compliance.

If controls from the Governance, Risk, and Compliance (GRC) application are implemented to mitigate risk, then Calculated Score = (Inherent Score – Residual Score) \* [(100 – Compliance)/100] + Residual Score.

Thus Calculated Score = Residual Score only if Compliance with the controls is 100%. If the Calculated Score > Residual Score, the organization is not 100% compliant with the controls used to mitigate a risk. This means that the calculated score can never be less than the residual score or greater than the inherent score.

If controls from the Governance, Risk, and Compliance (GRC) application are not implemented to mitigate risk, then Calculated Score = Residual Score. If the residual score is not set, then Calculated Score = Inherent Score.

## Create or modify a risk criteria threshold - Legacy

Risk Criteria are the scoring values attributed to the likelihood that a risk will occur, and the significance to your organization if the risk does occur. Risk Criteria Thresholds allow you to define what is deemed a high/likely or low/unlikely score. You can create or modify risk criteria thresholds, as necessary.

Risk defines Risk Criteria Thresholds as follows.

Table 114: Risk Criteria Thresholds

Likelihood	Significance	Scores
1 = Extremely Unlikely	1 = Very Low	0-5 = Very Low
2 = Unlikely	2 = Low	6-10 = Low
3 = Neutral	3 = Moderate	11-15 = Moderate
4 = Likely	4 = High	16-20 = High
5 = Extremely Likely	5 = Very High	21-25 = Very High

**Note:** See [Risk scoring](#) for information how the scores of Risks are calculated.

1. Navigate to Risk Administration Risk Criteria Thresholds .
2. Select the threshold to modify or click New.
3. Fill in the fields on the form, as appropriate.

Name	Description
Label	Sets the name of the Risk Criteria Threshold (for example, Extremely Likely or Very Low).
Type*	Select Likelihood, Significance, or Score depending on which the new threshold will apply.
Max value*	Sets the max score for a threshold.  <b>Note:</b> The properties restrict the values of Likelihood and Significance to 1-10. Therefore it is not beneficial to create Likelihood or Significance thresholds for max values greater than 10 or Score thresholds for max values greater than 100.

**Note:** \* indicates a mandatory field.

4. Click Submit.

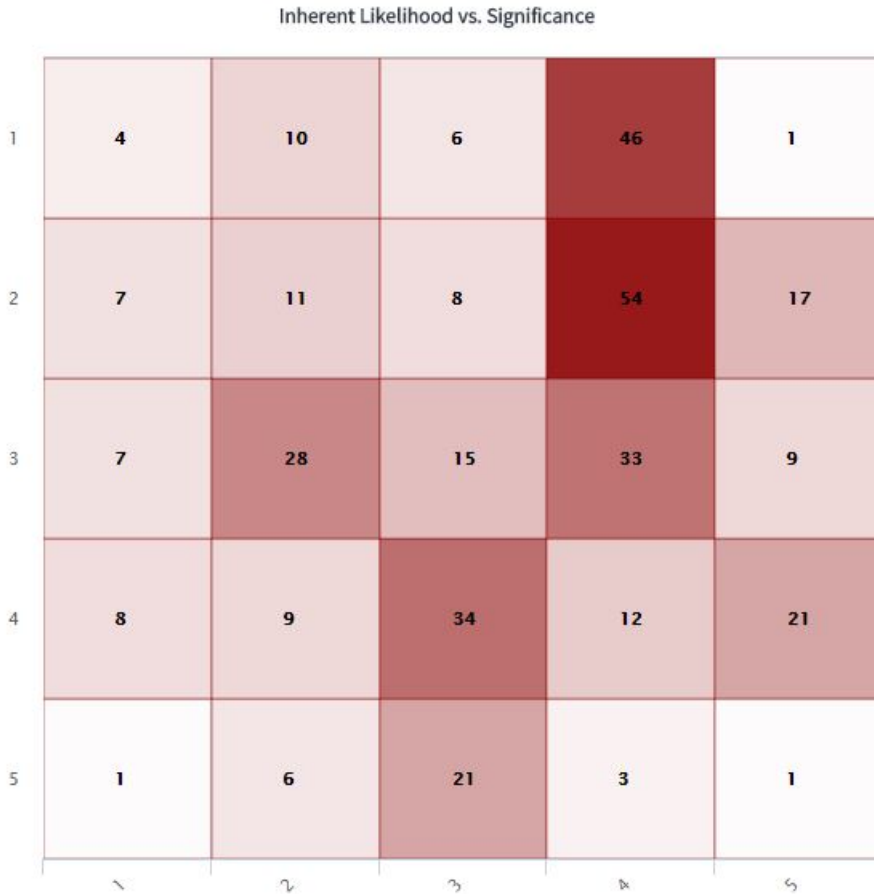
## Risk homepage - Legacy

The risk homepage provides an executive view into risk management, allowing risk managers to quickly identify areas of concern by pinpointing profiles with known high risk.

The overview displays warnings for profiles in non-compliance that increase risk. It also displays up-to-the minute information in gauges that contain valuable visuals such as the new Heatmap.

A Heatmap is a graphical representation of the number of records which meet a certain condition. The more records that meet a certain condition, the darker the color (the heat) is for that particular condition. In the case of Risk, the Heatmaps plot the values of likelihood vs. the values of significance. All Risks that meet a certain condition, for example Likelihood is 3 and Significance is 2, will aggregate into a score on the Heatmap. In the example Heatmap in the following image, the number of records that meet this condition is 8. Thus, using these Heatmaps, it is easy to identify the impact all Risks pose to

your organization. In the example below, heat in the bottom-right of the map means greater risk to the organization, showing risks that are both highly likely and highly significant, while heat in the upper-left of the map shows risk that is less likely and less significant.



**Figure 16: Example Heatmap**

The following gauges are provided out-of-box.

**Table 115: Out-of-box gauges**

Name	Visual	Description
Highest Risk Profiles	List	Display of any Profiles with a calculated score of moderate, high, and very high.
Risk Warnings	List	Display of any Profiles with a calculated score that is different (that is, greater) than the residual score, which allows users to quickly identify areas of non-compliance.

Name	Visual	Description
Risks by Response	Semi-donut	Chart of the number of risks that an organization has chosen to mitigate, avoid, accept, or transfer. User is able to drill-in to a list of all risks that meet a particular response.
Risks by Category	Semi-donut	Chart of the number of risks that apply to a particular category whether it be IT, Operational, Legal, Reputational, or Financial.
Inherent Likelihood vs. Significance	Heatmap	Plots the count of the number of risks by inherent likelihood vs. the inherent significance.
Residual Likelihood vs. Significance	Heatmap	Plots the count of the number of risks by residual likelihood vs. the residual significance. Ideally, all Risks would be in upper left corner of the plot (Likelihood = 1, Significance = 1).

## Risk properties - Legacy

The Administration module contains Properties. The Risk application provides properties associated with significance, likelihood, and application.

**Table 116: Risk properties**

Name	Description
Maximum value for Significance	Sets the maximum value (1-10) for significance on the risk criteria table. Decimals cannot be used, and are rounded if input. By default, the maximum is set to 5.
Maximum value for Likelihood	Sets the maximum value (1-10) for likelihood on the risk criteria table. Decimals cannot be used, and are rounded if input. By default, the maximum is set to 5.
A list of tables that are available in the Applies to field on forms	If this field is blank, all tables are available on the various forms for Profile Types, Profiles, and Risks. Defines a comma-separated list of tables that are available in the Applies to field on the Profile Type, Profile, and Risk form. Add .extended after the table name to include all extended tables.

## Activate Governance, Risk, and Compliance (GRC) - Legacy

Administrators can activate the Governance, Risk, and Compliance (GRC) plugin [com.snc.governance], and doing so automatically installs the Core GRC Components [com.snc.governance\_core] plugin. Additional plugins are activated as needed. This plugin provides demonstration data.

The Core GRC Components [com.snc.governance\_core] plugin includes components used by these plugins:

- Governance, Risk, and Compliance (GRC) [com.snc.governance]
- GRC: Risk [com.sn\_risk]
- Security Incident Response GRC support plugin [com.snc.security\_incident.grc]

These components include GRC Risks, Risk Criteria, Remediation Tasks, Policies, Standards, and Standard Operating Procedures.

---

**Note:** The Core GRC Components plugin does not include support for Authority Document management, Unified Compliance Framework (UCF) integration, Control management, Control testing, or Auditing Activities. To leverage these capabilities, install the Governance, Risk, and Compliance (GRC) [com.snc.governance] plugin.

---

1. Navigate to System Definition Plugins .
2. Find and click the plugin name.
3. On the System Plugin form, review the plugin details and then click the Activate/Upgrade related link.

If the plugin depends on other plugins, these plugins are listed along with their activation status.

If the plugin has optional features that are not functional because other plugins are inactive, those plugins are listed. A warning states that some files are not installed. If you want the optional features to be installed, cancel this activation, activate the necessary plugins, and then return to activating the plugin.

4. If available, select the Load demo data check box.

Some plugins include demo data—sample records that are designed to illustrate plugin features for common use cases. Loading demo data is a good policy when you first activate the plugin on a development or test instance.

You can also load demo data after the plugin is activated by clicking the Load Demo Data Only related link on the System Plugin form.

5. Click Activate.

# Index

## A

- activate
  - Audit Management [115](#)
  - Policy and Compliance Management [6](#)
  - Risk Management [68](#)
- activity, create an
  - Audit Tasks [136](#)
- assessment designer [103](#)
- attestation designer [55](#)
- attestations
  - Controls [54](#), [102](#)
- Audit
  - installed components
    - tables [116](#)
- audit definition [185](#), [229](#)
- Audit Management
  - activate [115](#)
  - Audit Tasks module [136](#)
  - Audit Testing module [143](#)
  - description [115](#)
  - Engagement Overview [123](#)
  - Engagement Workbench [125](#)
  - Engagements module [126](#)
  - installed components
    - tables [116](#)
  - installed with [116](#)
  - Issues module [58](#), [105](#), [148](#)
  - Scoping module [31](#), [91](#), [131](#)
- Audit Managementbusiness rules
  - installed components [116](#), [117](#), [117](#), [118](#), [120](#), [120](#)
- Audit Managementclient scripts
  - installed components [116](#), [117](#), [117](#), [118](#), [120](#), [120](#)
- Audit Managementproperties
  - installed components [116](#), [117](#), [117](#), [118](#), [120](#), [120](#)
- Audit Managementroles
  - installed components [116](#), [117](#), [117](#), [118](#), [120](#), [120](#)
- Audit Managementscript includes
  - installed components [116](#), [117](#), [117](#), [118](#), [120](#), [120](#)
- Audit Tasks
  - activity, create an [136](#)
  - control test, create a [138](#)
  - from an engagement [138](#)
  - interview, create an [140](#)
  - walkthrough, create a [141](#)
- Audit Tasks module
  - Audit Management [136](#)
- Audit Testing
  - test plan, create a [144](#)
  - test template, create a [143](#)
  - test template, relate a [144](#)
  - to a policy [144](#)
- Audit Testing module
  - Audit Management [143](#)
- audits
  - activities for [233](#)
  - GRC process for [227](#)
  - instance of [231](#)

- observations of [234](#)
- authority documents
  - create [18](#)
  - deactivate [20](#)

## C

- calculated links in GRC
  - example
    - authority document [204](#), [262](#)
    - generating links [266](#)
    - policy [262](#)
    - redirecting links [271](#)
  - explained [259](#)
  - tables for [260](#)
- citation deactivation
  - compliance [18](#)
- citations
  - creating [15](#), [204](#)
  - deleting [253](#)
  - imported from UCF [253](#)
  - relationships between [207](#)
  - relationships types [210](#)
  - view relationships [211](#)
- Compliance module
  - Policy and Compliance Management [13](#)
- configure
  - Policy and Compliance Management [7](#)
  - Risk Management [68](#)
- control test definitions
  - advanced conditions [180](#)
  - basic conditions [182](#)
  - condition collections [174](#)
  - condition collections, creating [175](#)
  - conditions for condition collections [175](#)
  - creating [176](#)
  - creating supporting data [180](#)
  - introduction to [223](#)
  - template conditions [184](#)
- control test, create a [138](#)
- control, add a
  - to a risk [101](#)
- control, create a
  - Controls [49](#)
- controls
  - creating in GRC [216](#)
  - introduction to [214](#)
  - super controls
    - viewing in email notification [223](#)
    - viewing in UCF document [219](#)
    - viewing in UCF update approvals [221](#)
    - viewing in UCF update request [220](#)
- Controls
  - attestations [54](#), [102](#)
  - control, create a [49](#)
- Controls module
  - Policy and Compliance Management [49](#)

- create
  - authority documents [18](#)
- create a
  - risk [96](#)
  - risk framework [90](#)
  - risk statement [88](#)
- create an
  - engagement [128](#)
- create risk [279](#)
- create Risk Criteria Threshold [173](#), [282](#)

## D

- deactivate
  - authority documents [20](#)
- description
  - Audit Management [115](#)
  - Policy and Compliance Management [5](#)
  - Risk Management [78](#)

## E

- engagement
  - create an [128](#)
- Engagement Overview
  - Audit Management [123](#)
- Engagement Workbench
  - Audit Management [125](#)
- Engagements module
  - Audit Management [126](#)

## F

- from a profile [32](#), [92](#), [133](#)
- from an engagement [138](#)

## G

- generate a risk [279](#)
- governance, risk, and compliance
  - adding relationships between citations [207](#)
  - audit activities [233](#)
  - audit instance [231](#)
  - audit observations [234](#)
  - audits [227](#)
  - authority documents [204](#)
  - available reports [188](#)
  - business rules [160](#)
  - calculated links [259](#)
  - calculated links example
    - authority document [204](#), [262](#)
    - generating links [266](#)
    - policy [262](#)
    - redirecting links [271](#)
  - calculated links tables [260](#)
  - calculated links, explained [259](#)
  - citations
    - creating [15](#), [204](#)
    - deleting [253](#)
    - imported from UCF [253](#)
    - relationship types [210](#)

- view relationships between [211](#)
- client scripts [158](#)
- control test definitions
  - advanced conditions [180](#)
  - basic conditions [182](#)
  - condition collections [174](#)
  - condition collections, creating [175](#)
  - conditions for condition collections [175](#)
  - supporting data [180](#)
  - template conditions [184](#)
- controls [214](#)
- controls, creating [216](#)
- creating [176](#)
- customizing reports [199](#)
- define a policy [212](#)
- define scope [173](#)
- installed components [153](#)
- interpreting reports [198](#)
- policies [212](#)
- reporting [187](#)
- risk approach rules [202](#)
- risk criteria [186](#), [200](#)
- risk definition [199](#)
- risks [199](#)
- script includes [158](#)
- super controls
  - viewing in email notification [223](#)
  - viewing in UCF documents [219](#)
  - viewing in UCF update approvals [221](#)
  - viewing in UCF update request [220](#)
- tables [153](#)
- UCF
  - approving document requests [245](#)
  - authority documents [36](#)
  - background processes [256](#)
  - configuring automatic downloads [253](#)
  - downloading files [235](#)
  - ignoring date changes when updating [172](#)
  - import process [235](#)
  - import properties [171](#)
  - manual updates [250](#)
  - selecting content to import [238](#)
  - version control [248](#)
- user roles [156](#), [170](#)
- vendor non-disclosure agreements
  - certification filter for [225](#)
  - certification template for [226](#)
  - modifying the control test definition [223](#)
  - vendor audit [230](#)

Governance, risk, and compliance

- GRC [4](#)

Governance, Risk, and Compliance

- activating [165](#), [286](#)

GRC: Profiles

- profile types, create [275](#)
- profile types, use [276](#)

GRC: Risk

- installed components
  - business rules [169](#)
  - properties [166](#)
  - roles [167](#)
  - script includes [168](#)



tables [166](#)  
 installed with [166](#)  
 roles [169](#)

## H

Heatmap [283](#)  
 homepage [283](#)

## I

indicator template, create an  
   Indicators [62](#), [109](#), [147](#)  
 indicator, add an  
   to a risk [100](#)  
 indicator, create an  
   Indicators [60](#), [108](#), [145](#)  
 Indicators  
   indicator template, create an [62](#), [109](#), [147](#)  
   indicator, create an [60](#), [108](#), [145](#)  
 installed with  
   Audit Management [116](#)  
   Policy and Compliance Management [7](#)  
   Risk Management [68](#)  
 interview, create an  
   Audit Tasks [140](#)  
 issue, create an  
   Issues [58](#), [106](#), [149](#)  
 Issues  
   issue, create an [58](#), [106](#), [149](#)  
 Issues module  
   Audit Management [58](#), [105](#), [148](#)  
   Policy and Compliance Management [58](#), [105](#), [148](#)  
   Risk Management [58](#), [105](#), [148](#)  
 IT governance, risk, and compliance  
   GRC process [170](#)

## L

Legacy GRC  
   migrate from [152](#)  
   migration [152](#)  
   migration, supported [152](#)  
   migration, unsupported [153](#)  
 Legacy Risk  
   migrate from [275](#)  
   migration [152](#)

## M

Managing Audits [228](#)  
 migrate from  
   Legacy GRC [152](#)  
   Legacy Risk [275](#)  
 migration, supported  
   Legacy GRC [152](#)  
 migration, unsupported  
   Legacy GRC [153](#)

## O

overview [274](#)  
 Overview  
   Risk Management [78](#)

## P

policies  
   defining in governance, risk, and compliance [212](#)  
   in governance, risk, and compliance [212](#)  
   scope of [173](#)  
 Policies and Procedures  
   approve, create a [23](#)  
   approve, retire a [24](#)  
   policy approval [24](#)  
   policy statement, create a [25](#)  
   policy statement, deactivate [30](#)  
   policy statement, relate a [16](#), [28](#), [28](#)  
   policy, create a [21](#)  
   policy, review a [23](#)  
   to a citation [16](#), [28](#)  
   to a policy [28](#)  
 Policies and Procedures module  
   Policy and Compliance Management [20](#)  
 policy and compliance  
   citation  
     deactivate [18](#)  
 Policy and Compliance Management  
   activate [6](#)  
   Compliance module [13](#)  
   configure [7](#)  
   Controls module [49](#)  
   description [5](#)  
   installed with [7](#)  
   Issues module [58](#), [105](#), [148](#)  
   Policies and Procedures module [20](#)  
   Scoping module [31](#), [91](#), [131](#)  
 Policy and Compliance Managementbusiness rules  
   installed components [7](#), [8](#), [9](#), [10](#), [10](#), [11](#)  
 Policy and Compliance Managementclient scripts  
   installed components [7](#), [8](#), [9](#), [10](#), [10](#), [11](#)  
 Policy and Compliance Managementproperties  
   installed components [7](#), [8](#), [9](#), [10](#), [10](#), [11](#)  
 Policy and Compliance Managementroles  
   installed components [7](#), [8](#), [9](#), [10](#), [10](#), [11](#)  
 Policy and Compliance Managementscript includes  
   installed components [7](#), [8](#), [9](#), [10](#), [10](#), [11](#)  
 Policy and Compliance Managementscripts  
   installed components [7](#), [8](#), [9](#), [10](#), [10](#), [11](#)  
 policy approval  
   Policies and Procedures [24](#)  
 policy statement, create a  
   Policies and Procedures [25](#)  
 policy statement, deactivate  
   Policies and Procedures [30](#)  
 policy statement, relate a [16](#), [28](#), [28](#)  
 policy, approve a  
   Policies and Procedures [23](#)  
 policy, create a  
   Policies and Procedures [21](#)

- policy, retire a
  - Policies and Procedures [24](#)
- policy, review a
  - Policies and Procedures [23](#)
- profile type, create a
  - Scoping [31](#), [91](#), [132](#)
- profile types
  - create [275](#)
  - use [276](#)
- profile, generate a [32](#), [92](#), [133](#)
- profile, reactivate
  - Scoping [34](#), [94](#), [135](#)
- properties [285](#)

## R

- relate Risk Definitions to Profile Types [279](#)
- reporting
  - customizing in GRC [199](#)
  - GRC portals [187](#)
  - GRC reports [188](#)
  - interpreting in GRC [198](#)
- risk
  - create a [96](#)
- Risk
  - create Risk Criteria Threshold [173](#), [282](#)
  - create Risk Definitions [278](#)
  - create risks [279](#)
  - generate a risk [279](#)
  - homepage [283](#)
  - installed components
    - business rules [169](#)
    - properties [166](#)
    - roles [167](#), [169](#)
    - script includes [168](#)
    - tables [166](#)
  - installed with [166](#)
  - overview [274](#)
  - properties [285](#)
  - relate Risk Definitions to Profile Types [279](#)
  - Risk Criteria Threshold, create [173](#), [282](#)
  - Risk Definitions, create [278](#)
  - score risk on Profiles [278](#)
  - score risks [282](#)
- Risk Definitions
  - create [278](#)
- risk framework
  - create a [90](#)
- Risk Library module
  - Risk Management [88](#)
- Risk Management
  - activate [68](#)
  - configure [68](#)
  - description [78](#)
  - installed with [68](#)
  - Issues module [58](#), [105](#), [148](#)
  - Overview [78](#)
  - Risk Library module [88](#)
  - Risk Register module [95](#)
  - Scoping module [31](#), [91](#), [131](#)
- Risk Managementbusiness rules
  - installed components [69](#), [69](#), [70](#), [73](#), [75](#), [76](#)

- Risk Managementclient scripts
  - installed components [69](#), [69](#), [70](#), [73](#), [75](#), [76](#)
- Risk Managementproperties
  - installed components [69](#), [69](#), [70](#), [73](#), [75](#), [76](#)
- Risk Managementroles
  - installed components [69](#), [69](#), [70](#), [73](#), [75](#), [76](#)
- Risk Managementscript includes
  - installed components [69](#), [69](#), [70](#), [73](#), [75](#), [76](#)
- Risk Managementscripts
  - installed components [69](#), [69](#), [70](#), [73](#), [75](#), [76](#)
- Risk Register
  - risk, generate a
    - from a profile type [95](#)
    - from a risk [96](#)
    - from a risk statement [96](#)
- Risk Register module
  - Risk Management [95](#)
- risk statement
  - create a [88](#)
- risk, generate a
  - from a profile type [95](#)
  - from a risk [96](#)
  - from a risk statement [96](#)
- risks
  - approach rules [202](#)
  - defining in GRC [199](#)
  - GRC [199](#)
  - GRC criteria [186](#), [200](#)

## S

- Scoping
  - from a profile [32](#), [92](#), [133](#)
  - profile type, create a [31](#), [91](#), [132](#)
  - profile, generate a [32](#), [92](#), [133](#)
  - profile, reactivate [34](#), [94](#), [135](#)
- Scoping module
  - Audit Management [31](#), [91](#), [131](#)
  - Policy and Compliance Management [31](#), [91](#), [131](#)
  - Risk Management [31](#), [91](#), [131](#)
- score risk on Profiles [278](#)
- score risks [282](#)

## T

- test plan, create a
  - Audit Testing [144](#)
- test template, create a
  - Audit Testing [143](#)
- test template, relate a [144](#)
- to a citation [16](#), [28](#)
- to a policy [28](#), [144](#)
- to a risk
  - control, add a [101](#)
  - indicator, add an [100](#)

## U

- UCF
  - download files [45](#)
- Unified Compliance Framework (UCF)
  - approving document requests [245](#)

- authority documents [36](#)
- citations, imported from
  - deleting [253](#)
- configuring automatic downloads [253](#)
- download [45](#)
- download background processes [256](#)
- downloading [235](#)
- ignoring date changes when updating GRC [172](#)
- import process [235](#)
- import properties [171](#)
- manually updating GRC [250](#)
- selecting content to import [238](#)
- version control in GRC [248](#)

## V

- vendor non-disclosure agreements
  - certification filter for [225](#)
  - certification template for [226](#)
  - modifying the control test definition [223](#)
  - vendor audit [230](#)

## W

- walkthrough, create a
  - Audit Tasks [141](#)